

Gegevensverwerking voor de juiste zorg op de juiste plek

Onderzoek Programma JuMP

Onderzoek in opdracht van NVZ
Januari 2022

Inhoudsopgave

1.	Het onderzoek	3
1.1	Inleiding	3
1.2	Onderzoeksvraag	3
1.3	Doelstellingen	4
1.4	Service evaluation	5
1.5	Scope van het onderzoek.....	5
1.6	Uitvoering	6
1.7	Leeswijzer	6
2.	Toetsingskader.....	7
2.1	Wet en regelgeving	7
2.2	Onderzoek naar aanknopingspunten voor gegevensverwerking	7
3.	Toets van voorgenomen verwerkingen	9
3.1	Inleiding	9
3.2	Onderzoeksvragen en doelstellingen.....	9
3.3	Beoordeling beoogde gegevensverwerkingen.....	10
3.4	Concrete voorbeelden	15
3.5	Service evaluation	19
3.6	Mogelijke andere routes.....	20
4.	Conclusies en aandachtspunten	21
4.1.	Doeleinden voor verwerking.....	21
4.2	Verwerkingsverantwoordelijke en verwerker.....	22
4.3	Grondslag en noodzakelijke verwerking	22
4.4	Beveiliging van gegevens	23
4.5	Privacybeleid en rechten betrokkenen	23
4.6	Geheimhouding	24
4.7	Slotconclusie	24
Bijlage 1	Uitwerking Toetsingskader	25
1.1	Wet op de geneeskundige behandelingsovereenkomst.....	25
1.2	De Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG ..	27
1.3	De Uitvoeringswet AVG (UAVG).....	34
1.4	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) ..	34
1.5	Wet Publieke Gezondheid (WPG)	37
1.6	Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg (Wegiz).....	37
1.7	Wkkgz.....	38

1. Het onderzoek

1.1 Inleiding

Vanuit het programma JuMP heeft de NVZ PrivacyCare gevraagd onderzoek te doen naar de mogelijkheden om gegevens te kunnen delen door zorgaanbieders met hun regiopartners ten behoeve van juiste zorg op de juiste plek binnen de kaders van de huidige privacywetgeving.

Programma JuMP

Toekomstbestendige medisch specialistische zorg, waarbij de patiënt de juiste zorg krijgt op de plek en manier die het beste bij hem past. Dat is waar de NVZ en haar leden aan werken met het programma JuMP: Juiste Medisch Specialistische Zorg voor de Patiënt. Met zorg wordt in dit kader bedoeld zowel het primaire zorgproces (de directe zorgverlening) als het organiseren, coördineren, afstemmen en evalueren van zorgactiviteiten.

Met het programma JuMP zetten ziekenhuizen en revalidatie-instellingen zich in de periode 2018 - 2022 extra in om samen met samenwerkingspartners juiste zorg op de juiste plek (JZOJP) te realiseren. Het delen van gegevens/data voor diverse doeleinden in de zorg is essentieel. Aan de ene kant wordt gestreefd naar integraal werken, over de schotten heen, samen bepalen wat de patiënt aan zorg en ondersteuning nodig heeft en wie dat het beste kan doen. Aan de andere kant kunnen de verschillende betrokken partijen de beschikbare informatie over de patiënt niet zomaar met elkaar delen op grond van wetgeving.

Binnen het programma JuMP hebben de NVZ-leden aangegeven belemmeringen te ervaren bij het delen van data over patiënten(groepen) met samenwerkingspartners¹ uit de regio. Om doelgroepen binnen een bepaalde populatie te kunnen identificeren, en om kenmerken van de regionale populatie in beeld te brengen, is er behoefte aan duidelijkheid over de mogelijkheden voor het gebruik van patiënten data.

Uit de JuMP-scan blijkt dat er interpretatieverschillen over privacywetgeving bestaan tussen organisaties, wat maakt dat het ontwikkelen van een regio-aanpak en de evaluatie van verbetertrajecten stagneert.

In dit onderzoek wordt in kaart gebracht welke van de gewenste gegevensverwerkingen om de doeleinden van JuMP te bereiken, mogelijk zijn en welke voorwaarden en waarborgen daar voor gelden.

1.2 Onderzoeksvraag

In het onderzoek staan de volgende vragen centraal:

1. Welke data over patiënten mogen onder welke voorwaarden worden gedeeld, als het gaat om de ontwikkeling van regioplannen en het evalueren van samenwerkingsprojecten?

¹ Andere zorgaanbieders waarmee wordt samengewerkt.

2. Welke data over patiënten mogen, onder welke voorwaarden, worden gedeeld als het gaat om voorkomen van zorg of het verlenen van pro-actieve zorg of het uitvoeren van preventieve interventies (zie ook de geformuleerde doelstellingen)?
3. Welke wetgeving is hierop (vraag 1 en 2) van toepassing en waar liggen de wettelijke grenzen? Waar liggen de (gepercipieerde) problemen?
4. Wat zijn goede praktijkvoorbeelden waarin data wordt gedeeld binnen de grenzen van de privacywetgeving zover hier relevant?

1.3 Doelstellingen

Toegespitst op het programma JuMP zijn er twee doelstellingen:

1. Om JZOJP te realiseren, is het noodzakelijk de regionale uitdagingen te identificeren en te prioriteren. Hiervoor is het noodzakelijk om doelgroepen (bijvoorbeeld kwetsbare ouderen) per zorgcategorie te definiëren.
In aanvulling op de beschikbare regiobeelddata van het RIVM moeten per regio populatiekenmerken in kaart worden gebracht, bijvoorbeeld leeftijd en aandoeningen. Zo kunnen de samenwerkingspartners in de regio de (toekomstige) zorgvraag, het zorgaanbod en de specifieke regionale knelpunten die daarbij kunnen ontstaan scherp krijgen.
Het moet daarom voor alle samenwerkende regiopartijen duidelijk zijn: welke (gezondheids)data mogen voor deze doeleinden worden gebruikt, en op welke wijze? Bijvoorbeeld: huisartsen hebben data over het percentage mensen met diabetes dat goed gereguleerd is. Mag je deze (populatie)data uit een regio bijeen brengen en gebruiken voor beleidsontwikkeling? En nog een laag dieper richting proactieve zorg: ziekenhuizen kunnen in kaart brengen hoeveel 70+ patiënten meerdere keren de SEH bezoeken. Dit zijn hoog-risico ouderen. Mag deze data met huisartsen gedeeld worden zodat zij gerichte, preventieve interventies kunnen inzetten?
2. Daarnaast is er behoefte aan het continu monitoren en evalueren van de (gezamenlijke) zorgactiviteiten van de betrokken regiopartijen. Partijen willen uitkomsten/kwaliteit van de zorg delen om te kunnen leren en verbeteren, en moeten daartoe data kunnen uitwisselen.
Ook de uitkomsten van samenwerkingsprojecten moeten kunnen worden uitgewisseld, zodat best practices én verbeterpunten kunnen worden geïdentificeerd². Om inzicht te krijgen in hoe patiënten door het systeem stromen, moeten persoonlijke data (met ID) aan elkaar gekoppeld worden. Na die koppeling kunnen de data geanonimiseerd worden voor analyse.
Om dit te kunnen doen is het noodzakelijk om te weten wat er binnen de bestaande regelgeving mogelijk is, en welke oplossingsrichtingen er zijn om deze data te kunnen delen.

²Voorbeeld: specialisGsch wondcentrum van ziekenhuis zet expertise in bij huisartsenpraktijk voor triage en gericht advies. Groot deel van de patiënten kan daardoor in eerste lijn blijven. Vervolgens moet men kunnen evalueren of patiënten uit de eerste lijn niet alsnog in het wondcentrum belanden en zo ja, na hoeveel weken (om te monitoren of verwijlsprotocol wordt nageleefd).

Concrete voorbeelden

Naast het beantwoorden van de vragen die uit de doelstellingen volgen zal een aantal concrete voorbeelden, benoemd door ziekenhuizen, als voorbeelden worden benoemd bij de beschrijving van mogelijkheden voor uitwisseling. Deze voorbeelden zijn opgenomen in hoofdstuk 3. Het Deventer ziekenhuis, Alrijne en het Flevoziekenhuis hebben aangegeven informatie te willen delen ten behoeve van het onderzoek.

1.4 Service evaluation

Indien uit het onderzoek blijkt dat er sprake is van een juridisch probleem op het gebied van uitwisseling onder de genoemde doelstellingen, vindt NVZ het interessant om te bestuderen of Service evaluation zoals in het Verenigd Koninkrijk ingezet, een mogelijkheid voor de Nederlandse omgeving is. In het VK maakt men juridisch onderscheid tussen wetenschappelijk onderzoek (met alle wettelijke eisen en voorwaarden) en de zogenoemde 'service evaluation'. Voor deze data analyse op populatie niveau zou volgens NVZ geen individuele toestemming nodig zijn. "Er zijn wel regels van toepassing ten aanzien van de zorgvuldigheid van gebruik van de data. Dit stelt regio's in staat om gezamenlijk, op basis van data, prioriteiten te benoemen en om initiatieven te monitoren en evalueren", zo geeft NVZ aan. Dit maakt het ook mogelijk om (in tegenstelling tot wetenschappelijk onderzoek) door snelle evaluatie, initiatieven tijdig bij te kunnen sturen. Dit draagt bij aan innovatie en kwaliteit van zorg.

Regionale best practices

Uit de inventarisatie in de regio's kunnen de 'lessons learned' en eventuele best practices worden gedestilleerd ten behoeve van de andere regio's. Deze worden beschreven. In dat kader wordt in elk geval gekeken naar de methode die wordt toegepast voor GGDH: Gezond en Gelukkig Den Haag – dataonderzoeksproject Gezond en Gelukkig Den Haag. Er wordt in het onderzoek bekeken of deze methode bruikbaar is voor andere casus en welke wettelijke basis daarvoor is.

Deze rapportage kan als handvat worden ingezet bij samenwerking t.b.v. de NVZ leden. De rapportage geeft antwoord op de onderzoeksvragen en doelstellingen en doet aanbevelingen.

1.5 Scope van het onderzoek

Wetenschappelijk onderzoek als grondslag valt in beginsel buiten de scope van dit onderzoek. Hiervoor bestaan al (duidelijke) regels. Ook is er een gedragscode beschikbaar, waarvan een herziene versie in ontwikkeling is. Wel wordt er in het onderzoek gekeken wanneer deze grondslag voor gegevensverwerking (mede) gebruikt kan worden voor het verwezenlijken van enkele doelstellingen in het programma. Te denken valt dan bijvoorbeeld aan het inschakelen van het CBS bij een verwerking, vanwege de bijzondere positie en bevoegdheden.

Als het gaat over samenwerkingsprojecten dan is in principe elke samenwerking die door de ziekenhuizen regionaal met andere zorgaanbieders wordt aangegaan i.v.m. de juiste zorg op de juiste plaats bedoeld. Zover samenwerkingsprojecten zien op het inrichten van *vroegsignalering* in het algemeen (dus in het algemeen ten aanzien van een bepaalde populatie met bepaalde kenmerken) ten behoeve van het kunnen leveren van de juiste zorg op de juiste plek en het voorkomen van te laat ingrijpen en onnodige zorg, zullen deze niet in deze fase van het onderzoek worden betrokken, teneinde de omvang en overzichtelijkheid ervan te

waarborgen. Er is besproken met NVZ dat dit aspect in een tweede fase zo gewenst uitgewerkt kan worden omdat ook dit aspect heel relevant en actueel wordt geacht.

1.6 Uitvoering

Het onderzoek is uitgevoerd binnen de in de opdracht gestelde kaders.

Voor uitvoering zijn de door opdrachtgever aangeleverde documenten zoals de opdrachtomschrijving en de documentatie, gesprekken met de zorgaanbieders en klankbordgroep en ingebrachte casus uit de ziekenhuizen uitgangspunt voor het onderzoek. Nadere informatie is per mail en in interviews gegeven. Het onderzoek is uitgevoerd door PrivacyCare.

1.7 Leeswijzer

Hoofdstuk 2 geeft het toetsingskader voor het onderzoek (uitgebreid uitgewerkt in de bijlage) en een beschrijving van de op verzoek van NVZ nader onderzochte wetten. Hoofdstuk 3 beschrijft de grondslagen en mogelijkheden voor gewenste gegevensverwerkingen. Hoofdstuk 4 beschrijft een aantal aandachtspunten en vat de bevindingen samen. Een uitwerking van het juridisch kader is in de bijlage opgenomen.

2. Toetsingskader

2.1 Wet en regelgeving

Het verwerken van gegevens van patiënten en cliënten in de regionale zorg valt onder de werking van de Algemene verordening gegevensbescherming (AVG). Deze Europese wetgeving vormt de algemene basis voor inrichting van de gegevensverwerking. Enkele bijzondere wetten geven daaraan een specifieke invulling.

De Uitvoeringswet AVG (UAVG) geeft voor sommige regels uit de AVG een nadere uitwerking voor lidstaat Nederland. Voor zorgprofessionals geldt naast de AVG de WGBO en de Wet BIG, waarin o.a. de dossierplicht en het beroepsgeheim voor zorgprofessionals geregeld is. Deze bepalingen zorgen voor een verzwaring van het regime wanneer het gaat om het verwerken van persoonsgegevens die afkomstig zijn uit het dossier en waarop de geheimhoudingsplicht rust. Deze bepalingen gelden voor zorgverleners en zorgaanbieders in het kader van behandeling, en voor BIG geregistreerde hulpverleners.

Regels over het verwerken van het BSN zijn vervat in de Wet algemene bepalingen burgerservicenummer (Wabb) en in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

Sinds 2017 is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabpvz) van kracht, waarvan enkele bepalingen uiteindelijk niet in werking zijn getreden. Deze wet regelt het toestemmingsvereiste voor het elektronisch uitwisselen van cliëntgegevens tussen zorgaanbieders. Op diverse terreinen gelden ook andere wetten die bepalingen over gegevensverwerking bevatten, zoals de Jeugdwet, de WMO 2015. Deze wetten worden alleen in het onderzoek betrokken waar dat relevant is voor een concrete casus.

Voor de leesbaarheid is de uitwerking van het toetsingskader in een bijlage opgenomen (Bijlage 1).

2.2 Onderzoek naar aanknopingspunten voor gegevensverwerking

Naast het beschrijven van de kaders van de WGBO, de (U)AVG en deels de Wabvpz, wordt in de onderzoeksopdracht gevraagd om te verkennen of de Wet Publieke Gezondheid (WPG) ruimte biedt voor bepaalde gegevensuitwisseling, in het kader van de volksgezondheid. Ook de relatie met het Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg (Wegiz) en de Wkkgz is uitgewerkt in het toetsingskader van dit onderzoek (bijlage 1). De WPG, Wegiz en Wkkgz bieden geen extra grondslagen voor persoonsgegevensverwerking in het kader van dit onderzoek.

In de (regionale) zorg hebben gemeenten soms ook een rol. Door JuMP wordt waar mogelijk aansluiting gezocht bij het wetsvoorstel Wet aanpak meervoudige problematiek sociaal domein (Wams). Met dit wetsvoorstel wordt de huidige Wet maatschappelijke ondersteuning 2015 (Wmo 2015) aangepast. Dit wetsvoorstel is vorig jaar in consultatie geweest en er zijn diverse wijzigingsvoorstellen op gekomen. Het kan nog even duren voor een aangepast wetsvoorstel naar de Kamers gaat. Dit wetsvoorstel moet bijdragen aan een betere zorg voor inwoners met meervoudige problematiek. Het wetsvoorstel wil daarvoor een duidelijke taak regelen voor gemeenten om in concrete gevallen te komen tot een integrale en gecoördineerde aanpak en wil meer duidelijkheid geven over het verwerken van persoonsgege-

vens tussen betrokken instanties. Ook wordt de mogelijkheid van hergebruik van gegevens door de gemeente, van gegevens uit de verschillende domeinen waarover zij beschikt, geregeld.

Bijna alle gemeenten kennen een meldpunt waar burgers en professionals terecht kunnen met zorgen over gezondheid, het welzijn, de zelfredzaamheid of participatie van zichzelf of een ander. Om een goede behandeling van de meldingen mogelijk te maken wordt met dit wetsvoorstel voorzien in een betere juridische basis voor de gegevensverwerking door de meldpunten. Het wetsvoorstel kan in de toekomst mogelijkheden bieden voor uitwisseling van bepaalde gegevens tussen ziekenhuizen en partners in het sociaal domein en het college van B en W. Het is te vroeg om dit nu precies te overzien en gelet op de vraagstelling in het onderzoek is de relevantie in deze fase beperkt.

Gevraagd is ook welke elementen voor regionale zorg uit het Handvat Gegevensuitwisseling Zorg en Veiligheid kunnen worden gebruikt bij zorgverlening en afstemming door regionale partijen. Dit aspect lijkt in de eerste fase van dit onderzoek niet voldoende relevant te zijn gelet op de onderzochte problematiek en vragen van de ziekenhuizen³. Daarin komen de actoren uit het veiligheidsdomein niet voor. Voor wat betreft de gemeente als actor wordt daar in het rapport op in gegaan. In een mogelijke tweede fase van het onderzoek waar ingezoomd zal kunnen worden op samenwerkingsprojecten ten behoeve van vroegsignalering, wordt uitgebreider aangesloten bij de wetgeving en handvatten uit het sociaal domein. Er is diverse wetgeving in voorbereiding om de mogelijkheden voor gegevensuitwisseling meer te laten aansluiten op de behoefte in het sociaal domein bij meervoudige problematiek.

³ Zie ook de aangedragen casuïstiek onder 3.4.

3. Toets van voorgenomen verwerkingen

3.1 Inleiding

In de onderzoeksopdracht zijn onderzoeksvragen, doelstellingen en casuïstiek uit de praktijk benoemd. De onderzoeksvragen zijn overkoepelend voor het onderzoek en worden in het rapport op verschillende plekken beantwoord. De doelstellingen, vanuit het programma JuMP geven nadere invulling aan de eerste twee algemeen geformuleerde onderzoeksvragen (zie hierna). Op de casuïstiek wordt apart ingegaan en deze praktijksituaties worden aan het einde van dit hoofdstuk besproken.

3.2 Onderzoeksvragen en doelstellingen

In deze onderzoeksopdracht staan de volgende vragen centraal:

1. Welke data over patiënten mogen onder welke voorwaarden worden gedeeld, als het gaat om de ontwikkeling van regioplannen en het evalueren van samenwerkingsprojecten?
2. Welke data over patiënten mogen, onder welke voorwaarden, worden gedeeld als het gaat om voorkomen van zorg of het verlenen van pro-actieve zorg of het uitvoeren van preventieve interventies (zie ook de geformuleerde doelstellingen)?
3. Welke wetgeving is hierop van toepassing en waar liggen de wettelijke grenzen? Waar liggen de (gepercipieerde) problemen?
4. Wat zijn goede praktijkvoorbeelden waarin data wordt gedeeld binnen de grenzen van de privacywetgeving zover hier relevant?

Doelstellingen

Toegespitst op het programma JuMP zijn er twee doelstellingen:

1. Om JZOJP te realiseren, is het noodzakelijk de regionale uitdagingen te identificeren en te prioriteren. Hiervoor is het noodzakelijk om doelgroepen (bijvoorbeeld kwetsbare ouderen) per zorgcategorie te definiëren. In aanvulling op de beschikbare regiobeelddata van het RIVM moeten per regio populatiekenmerken in kaart worden gebracht, bijvoorbeeld leeftijd en aandoeningen. Zo kunnen de samenwerkingspartners in de regio de (toekomstige) zorgvraag, het zorgaanbod en de specifieke regionale knelpunten die daarbij kunnen ontstaan scherp krijgen.

Het moet daarom voor alle samenwerkende regiopartijen duidelijk zijn: welke (gezondheids)data mogen voor deze doeleinden worden gebruikt, en op welke wijze? Bijvoorbeeld: huisartsen hebben data over het percentage mensen met diabetes dat goed gereguleerd is. Mag je deze (populatie)data uit een regio bijeen brengen en gebruiken voor beleidsontwikkeling? En nog een laag dieper richting proactieve zorg: ziekenhuizen kunnen in kaart brengen hoeveel 70+ patiënten meerdere keren de SEH bezoeken. Dit zijn hoog-risico ouderen. Mag deze data met huisartsen gedeeld worden zodat zij gerichte, preventieve interventies kunnen inzetten?

2. Daarnaast is er behoefte aan het continu monitoren en evalueren van de (gezamenlijke) zorgactiviteiten van de betrokken regiopartijen. Partijen willen uitkomsten van de zorg delen om te kunnen leren en verbeteren, en moeten daartoe data kunnen uitwisselen. Ook de uitkomsten van samenwerkingsprojecten moeten kunnen worden uitgewisseld, zodat best practices én verbeterpunten kunnen worden geïdentificeerd. Om inzicht te krijgen in hoe patiënten door het systeem stromen, moeten persoonlijke data (met ID) aan elkaar gekoppeld worden. Na die koppeling kunnen de data geanonimiseerd worden voor analyse.

Om dit te kunnen doen is het noodzakelijk om te weten wat er binnen de bestaande regelgeving mogelijk is, en welke oplossingsrichtingen er zijn om deze data te kunnen delen.

3.3 Beoordeling beoogde gegevensverwerkingen

Onderzoeksvragen 1 en 2 omvatten samen de kern vraagstelling van het onderzoek. Aan de hand van de geformuleerde doelstellingen worden deze vragen beantwoord evenals met de beantwoording van de casuïstiek. Daarnaast wordt waar mogelijk samenvattend aangegeven in algemene termen welke data onder welke voorwaarden gedeeld mogen worden gelet op de doelstellingen van JuMP.

Onderzoeksvraag 3 is in hoofdstuk 2 Het juridisch kader, in algemene termen beantwoord door de reikwijdte van de verschillende wetten te beschrijven en komt concreet in dit hoofdstuk aan de orde per onderdeel van de beoogde verwerkingen voor zover dat relevant is. Onderzoeksvraag 4 wordt in hoofdstuk 4 besproken.

Onderzoeksvragen 1 en 2 gaan over het verwerken van gegevens voor verschillende doeleinden. Die doeleinden zijn:

- Ontwikkelen van regioplannen (zorgplanning en beleid)
- Evalueren van samenwerkingsprojecten
- Voorkomen van zorg
- Verlenen van proactieve zorg of uitvoeren van preventieve interventies

De bovenste twee doeleinden betreffen verwerkingen op geaggregeerd niveau, de onderste twee zijn gericht op persoonlijke zorg.

Onderzoeksvraag 1: Ontwikkeling en evaluatie

In onderzoeksvraag 1 gaat het om beschrijvingen uit doelstellingen 1 en 2. Zorgplanning en beleid zit in de eerste doelstelling en de evaluatie van samenwerkingsprojecten in de tweede. Deze doelstellingen sluiten nauw aan bij het uitvoeren van kwaliteitsonderzoek en meting. En secundair het bepalen van beleid en plannen op basis van het overzicht van de bestaande situatie.

Artikel 9 lid 1 van de AVG geeft een algemeen verbod op het verwerken van gezondheidsgegevens. Dit is echter niet van toepassing met uitdrukkelijke toestemming van de betrokkene (artikel 9 lid 2 sub a AVG), wanneer verwerking gebeurt in verband met het verlenen van gezondheidszorg of het beheer van de beroepspraktijk (artikel 9 lid 2 sub h AVG), dan wel als dit voor het behoud van hoge normen van kwaliteit nodig is op grond van het lidstatelijk of unierecht (artikel 9 lid 2 sub i AVG).

Een en nader is nader uitgewerkt in de UAVG.

Artikel 30.3 Uitvoeringswet AVG luidt, voor zover hier relevant, als volgt:

Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door:

- a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk;

Het begrip ‘beheer’ dient in dit onderdeel te worden uitgelegd als het waarborgen van de kwaliteit van de verleende zorg, intercollegiale toetsing door hulpverleners onderling (kwaliteitsbeheer) en de betaling van rekeningen voor medische behandeling. Daarbij dient een grondslag voor verwerking uit artikel 6 AVG te worden aangewezen (bijv. artikel 6 lid 1 sub b, sub a of sub f AVG).

Artikel 3 Wkkgz verplicht de zorgaanbieder tot het verlenen van goede zorg en het borgen van de kwaliteit die daartoe leidt. Artikel 7 Wkkgz geeft met name aan hoe de zorgaanbieder o.a. zorg draagt voor de naleving van artikel 3 Wkkgz. Het op systematische wijze verzamelen en registreren van gegevens betreffende de kwaliteit van zorg op een manier die vergelijking mogelijk maakt met andere zorgaanbieders is een opdracht tot het verwerken van die gegevens. De wet en het Uitvoeringsbesluit Wkkgz geven geen nieuwe verwerkingsgrondslagen voor het verwerken van persoonsgegevens voor dit doeleinde, dit wordt namelijk niet expliciet benoemd. Het gaat dus om gegevens die geanonimiseerd zijn uit het zorgproces, zoals kwaliteitsindicatoren.

De beste grondslag voor het verwerken van persoonsgegevens, zover noodzakelijk, voor kwaliteitsdoeleinden en beheer is op grond van het bovenstaande artikel 9 lid 2 sub h AVG, (jo. artikel 6 AVG), jo. artikel 30 lid 3 sub a UAVG. Deze grondslag biedt de mogelijkheid aan zorgaanbieders om gelet op de opdracht uit de Wkkgz en het beheer van de instelling of de beroepspraktijk, gegevens van patiënten uit dossiers te verzamelen voor nauw omschreven doelstellingen binnen dat kader. Dit mag alleen gebeuren door een medewerker van de instelling die aan het beroepsgeheim gehouden is (AVG/UAVG). Zodra de gegevens die benodigd zijn verzameld zijn moeten deze (one way) gepseudonimiseerd of geanonimiseerd⁴ worden, opdat herleiding naar de betrokkene voorkomen wordt. Het beheer van de beroepspraktijk geeft aan dat het niet alleen om beheer binnen de instelling hoeft te gaan. Dit beheer kan zich bijvoorbeeld uitstrekken tussen samenwerkende zorgaanbieders binnen een bepaald domein.

Omdat de WGBO ook eisen stelt gelet op de geheimhoudingsplicht, en de AVG verlangt dat verwerkingen achterwege blijven als de geheimhoudingsplicht daaraan in de weg staan, kunnen gegevens niet zomaar met derden worden gedeeld voor deze doeleinden.

De KNMG heeft zich ook gebogen over de vraag of herleidbare gegevensverwerking mogelijk is voor kwaliteitsdoeleinden. Op basis van de WGBO is toestemming van de patiënt vereist voor het verwerken van de gegevens uit het dossier aan een derde die niet onder de uitzonderingsgronden valt (zoals een rechtstreeks betrokkene bij de behandeling). Patiëntgegevens uit een EPD mogen voor kwaliteitsdoeleinden worden gebruikt, volgens de KNMG-richtlijn Omgaan met medische gegevens.

Medische gegevens van patiënten kunnen worden gebruikt voor kwaliteitsdoeleinden, zoals incidentmeldingen en kwaliteitsvisitaties. Het gebruik van de gegevens voor deze doelen ligt in het verlengde van het verlenen van goede zorg. De toestemming van de patiënt voor het gebruiken van gegevens voor deze kwaliteitsdoeleinden mag worden verondersteld.⁵

⁴ De techniek van pseudonimiseren en anonimiseren wordt in dit rapport vanwege omvang en scope niet uitgewerkt. Voor meer informatie zie onder andere www.CBS.nl.

⁵ KNMG-richtlijn Omgaan met medische gegevens 2021, pag.21

Paragraaf 8.2 van de richtlijn gaat dieper in op de mogelijkheid van veronderstelde toestemming:

“Voor kwaliteitsdoeleinden geldt dat artsen medische gegevens zoveel mogelijk moeten anonimiseren wanneer het niet noodzakelijk is dat zij tot de patiënt herleidbare gegevens gebruiken of verstrekken. Als het gaat om de toegang tot en het gebruik van medische gegevens die tot een patiënt herleidbaar zijn, geldt als hoofdregel dat hiervoor expliciete toestemming van die patiënt nodig is. Juristen gaan er veelal van uit dat dit anders ligt als deze medische gegevens worden gebruikt voor kwaliteitsdoeleinden, zoals bij incidentmeldingen en kwaliteitsvisitaties”.⁶

Het gebruik van de gegevens voor deze doelen ligt in het verlengde van het verlenen van goede zorg. Daarom kan worden aangenomen dat in die gevallen toestemming van de patiënt mag worden verondersteld, mits de gegevens uitsluitend voor kwaliteitsdoelen worden gebruikt. De patiënt moet wel de mogelijkheid hebben om bezwaar te maken tegen het gebruik van zijn gegevens voor kwaliteitsdoeleinden. Daarvoor moet de patiënt vooraf kennis hebben kunnen nemen van de mogelijkheid dat zijn gegevens voor kwaliteitsdoelen worden gebruikt.⁷

Als de patiënt hiertegen bezwaar maakt, mogen zijn gegevens niet gebruikt worden, tenzij in de wet een verplichting staat om patiëntgegevens in voorkomende gevallen voor kwaliteitsdoelen te gebruiken (die verplichting is er dus op grond van de Wkkgz niet voor herleidbare gegevens, maar wel voor bepaalde niet herleidbare gegevens, die vergeleken moeten kunnen worden met gegevens van andere zorgaanbieders).

"Een kwaliteitsvisitatie is een intercollegiale toetsing. Het doel van de visitatie is om de kwaliteit van de zorg te verbeteren. Het is een instrument voor een individuele arts of voor een groep artsen om hun functioneren te evalueren en daar feedback op te ontvangen. De visitatie wordt uitgevoerd door personen die zelf ook een geheimhoudingsplicht hebben. Een kwaliteitsvisitatie bestaat uit verschillende onderdelen. Een onderdeel kan zijn dat de kwaliteit van de dossiervoering, en daarmee van de verleende zorg, wordt geëvalueerd. Via een aselecte steekproef kan de visitatiecommissie patiëntendossiers selecteren en beoordelen. Deze dossierinzage beperkt zich tot het doel van de kwaliteitsvisitatie. Gegevens waaruit de identiteit van de patiënt kan worden herleid, worden zo veel mogelijk weggelaten."

Een zorgaanbieder is op grond van art. 2 en 7 Wkkgz ook verplicht tot het verlenen van goede zorg. De toestemming van patiënten kan daarom worden verondersteld mits zij vooraf daarover zijn geïnformeerd (het kenbaar is) en gelegenheid hebben gehad om daartegen bezwaar te maken, zo stelt de KNMG.

PrivacyCare sluit zich aan bij deze opvatting die breder gedeeld is onder gezondheidsrecht juristen. Wel is het van belang dat gegevens geanonimiseerd worden zodra dat mogelijk is en (niet herleidbaar) gepseudonimiseerd zolang dat voor het samenbrengen van gegevens nog van belang is.

⁶ Richtlijn KNMG, Omgaan met medische gegevens, pag 120. Momenteel worden regels ontwikkeld voor het mogen verstrekken van patiëntgegevens aan 'kwaliteitsregistraties'. Zie het Advies Commissie Governance van Kwaliteitsregistraties.

⁷ Richtlijn KNMG, Omgaan met medische gegevens, pag 122.

Uit de tekst van de richtlijn blijkt dat het een zachte norm is. De tekst 'juristen gaan er veelal vanuit' laat nog ruimte voor interpretatie. Zeker nu de voorgenomen verwerkingen tussen zorgaanbieders in de regio ruimer is dan een kwaliteitsvisitatie an sich. Wel wordt er gesproken van kwaliteitsdoeleinden in het algemeen, *zoals* kwaliteitsvisitaties. De Wkkgz is vrij ruim als het gaat om wat kwaliteitsonderzoek en borging inhoudt. Het gaat erom wat noodzakelijk is om de kwaliteit van de 'goede zorg' te borgen. Ook de ontheffing van artikel 30 UAVG geeft in de toelichting geen vormvereisten voor kwaliteitsdoeleinden die onder beheer vallen.

BSN

Hierbij is van belang te benoemen dat het verwerken van het BSN aan strikte grondslagen gebonden is. Dit mag alleen op grond van de wet of de doeleinden daarin genoemd. Tussen zorgaanbieders wordt het BSN uitgewisseld in verband met de goede zorgverlening. Beheer is als zodanig geen doeleinde dat is benoemd. Voor zover en zolang kwaliteitsborging voortvloeit uit of essentieel is voor het leveren van goede zorg, zou men kunnen redeneren dat de verwerking van het BSN geboden is. Wanneer is dat het geval en waar eindigt het? Om een veilig onderscheid te maken wordt geadviseerd om een splitsing te maken in kwaliteitsborging voor individuele zorgverlening en kwaliteitsbeheer voor een populatie. In het eerste geval is het gebruik van het BSN nog van belang om terug te kunnen gaan naar de patiënt. In het tweede geval gaat het vooral om uitkomsten van zorg en eventuele aanpassingen toepassen op de populatie al geheel. Dan zou gepseudonimiseerde of geanonimiseerde verwerking aangewezen zijn. Een geëncrypt BSN dat nog terug te herleiden is naar de betrokkene wordt beschouwd als het verwerken van het BSN. Alleen wanneer er sprake is van pseudonimisering conform de AVG, hoeft die verwerking door de verwerkingsverantwoordelijke niet te worden beschouwd als verwerking van het BSN (maar wel als het verwerken van persoonsgegevens).

Samenvattend

Het handvat is om voor dit doeleinde de noodzakelijke dataset (dataminimalisatie is vereist) uit het EPD te gebruiken voor kwaliteitstoetsing. Extractie gebeurt door een speciaal aangewezen kwaliteitsmedewerker met geheimhoudingsplicht. Gegevens in de instelling of zorgaanbieder kunnen samengebracht worden op basis van het BSN. Wanneer gegevens zo nodig worden gedeeld met een andere zorgaanbieder die de kwaliteitstoets tussen de ketenpartners of samenwerkingspartners uitvoert, dan zijn de gegevens (voor verstrekking) zoveel mogelijk geanonimiseerd, dan wel indien noodzakelijk voor samenbrengen van gegevens per patiënt, gepseudonimiseerd volgens daarvoor geldende hoge uitvoeringsstandaarden, zonder dat terughерleiding van het BSN mogelijk is. De verstrekte dataset is minimaal mogelijk, herleiding wordt zoveel mogelijk voorkomen door aanvullende maatregelen, zoals het aanpassen van datumvelden naar geaggregeerde waarden. Gegevens worden slechts zolang bewaard als nodig is voor de kwaliteitsdoeleinden. Daarna kunnen ze volledig anoniem (niet herleidbaar) worden bewaard. Voor patiënten is het kenbaar dat deze gegevensverwerking wordt uitgevoerd of mogelijk is, en als patiënten bezwaar maken worden van die patiënten geen direct of indirect herleidbare gegevens gebruikt.

Regioplannen

Ten aanzien van het tweede deel van de vraag: Als het gaat om het bepalen van beleid en het maken van regioplannen op basis van het overzicht van de bestaande situatie, gaat het

niet rechtstreeks om kwaliteitsdoeleinden. In de doelstellingen is verwoord welke gegevens en dataset nodig wordt geacht voor deze beleidsbeslissingen. Het gaat om het identificeren van bepaalde doelgroepen in bepaalde zorgcategoriën. Deze componenten hebben wel te maken met het beheer van de instelling, of beroepspraktijk voor zover het samenwerking betreft (regioplannen). Algemeen uitgangspunt van de AVG is echter dat voor beleids- en managementinformatie in beginsel niet herleidbare data wordt gebruikt. Regioplannen en het in kaart brengen van knelpunten zit op het snijvlak van kwaliteitsborging en planning. Van belang is om na te gaan welke gegevensvergelijking echt noodzakelijk is om de kwaliteit van goede zorg te kunnen waarborgen en welke gegevens nodig zijn om een vergelijking van incidentie en aantallen te maken. De eerste categorie gegevens zou conform het bovenstaande (voor kwaliteitsdoeleinden) kunnen worden verwerkt. De tweede categorie kan worden vergeleken op grond van niet herleidbare gegevens.

Het volgen van een persoon in de systemen van een instelling met het doel de persoon te oormerken als een 'kwetsbare oudere' of bijvoorbeeld een behandeling weigerende COPD'er is niet zomaar mogelijk. Om een persoon te volgen in zijn zorgtraject in de keten zal er toestemming moeten zijn van de patiënt. Veel patiënten zijn bereid toestemming te geven voor het delen van gegevens voor ketenzorg of extra aandacht door de instelling, zoals ouderen. En binnen een afdeling of ten behoeve van een behandeling door een afdeling (bijv hartpoli) volgen van een persoon kan vanzelfsprekend wel zonder toestemming. Dit wordt verwacht door de patient en is verondersteld. Oormerken of stigmatiseren ten behoeve van uitwisseling mag niet. Bepaalde kwaliteiten kunnen neutraal beschreven worden in het dossier en als er toestemming is om te volgen dan kunnen die kwaliteiten gemonitord worden. Een behandeling is echter nooit verplicht dus het niet behandelen wordt wel in het dossier genoteerd, maar het oormerken als een weigeraar (om dit te kunnen delen) is een ongewenste profilering.

Het volgen van een patiënt bij/door een zorgverlener of op één afdeling is doorgaans ten behoeve van de directe zorgverlening/behandeling aan de betrokkene, en kan in het kader van het uitvoeren van de behandeling worden beschouwd.

Uit de doelstellingen komt de vraag: huisartsen hebben data over het percentage mensen met diabetes dat goed gereguleerd is. Mag je deze (populatie)data uit een regio bijeen brengen en gebruiken voor beleidsontwikkeling? Deze data mag dus gelet op het bovenstaande samengebracht worden, en dit kan zonder gebruik te maken van herleidbare persoonsgegevens van patiënten.

Onderzoeksvraag 2: Voorkomen van zorg en verlenen van proactieve zorg en interventies

In de doelstellingen van het programma JuMP wordt het voorbeeld gegeven van ouderen: Ziekenhuizen kunnen in kaart brengen hoeveel 70+ patiënten meerdere keren de SEH bezoeken. Dit zijn hoog-risico ouderen. Mag deze data met huisartsen gedeeld worden zodat zij gerichte, preventieve interventies kunnen inzetten?

Van de patiënten wordt een dossier bijgehouden op de SEH. Het is mogelijk om vanuit de afdeling in een periode te bekijken welke patiënten meer dan eens geweest zijn. Dit kan in het kader van de normale patiëntenzorg gebeuren door de hulpverlener. Over het algemeen krijgt de huisarts van een patiënt na een bezoek aan de SEH een specialistenbrief met de conclusies van de behandeling. Die mag op basis van veronderstelde toestemming gestuurd

worden. Er is geen bezwaar om aan dezelfde huisarts, ten aanzien van dezelfde patiënt aan het einde van het jaar nog een specialistenbrief te sturen waarin aandacht wordt gegeven aan het meermaals bezoeken van de SEH. Dit is een activiteit die past in het kader van de goede uitvoering van de behandelingsovereenkomst.

Geaggregeerd kunnen deze data ook met de groep van huisartsen in de regio gedeeld worden voor preventieve interventies op populatieniveau.

In de richtlijn Omgaan met medische gegevens (pag 21) van de KNMG staat in de paragraaf over verwijzing en terugkoppeling:

"De ontvangende arts voegt de verwijsbrief (of de relevante delen daaruit) toe aan het medisch dossier van de patiënt. Met het oog op de kwaliteit en continuïteit van de zorg is het gebruikelijk dat een medisch specialist die een patiënt na een verwijzing heeft behandeld, de verwijzer op de hoogte stelt. Deze terugkoppeling gebeurt meestal via een specialistenbrief. Daarbij geeft de specialist een antwoord op de vraag die de verwijzer heeft gesteld. De medisch specialist mag de brief met veronderstelde toestemming van de patiënt naar de verwijzer sturen. In veel gevallen kan hij veronderstellen dat die toestemming er is, tenzij de patiënt daartegen bezwaar heeft gemaakt. De verwijzer neemt de specialistenbrief (of relevante delen daaruit) op in het dossier van de patiënt.

In de landelijke samenwerkingsafspraken tussen de GGZ en huisartsen wordt aanbevolen dat een behandelaar in de GGZ na een consultatie, de intake en bij het afsluiten van de behandeling alleen een terugkoppeling aan de huisarts mag geven als de patiënt hiervoor toestemming geeft.

3.4 Concrete voorbeelden

Er is een aantal concrete voorbeelden benoemd vanuit ziekenhuizen die als voorbeelden worden meegenomen in het onderzoek.

Voorbeeld 1. *Een ziekenhuis weet dat er jaarlijks 400 patiënten zijn met leeftijd 70+ die meer dan drie keer de SEH bezoeken per jaar.*

Kunnen deze data (gepseudonimiseerd) worden gekoppeld aan data over hoog risico patiënten huisarts / thuiszorg / gemeente om inzicht te genereren in hoeverre 'hoog risico' ook overeenkomt met 'veel SEH bezoek'?

Dit zelfde wordt nu al gedaan in het project GGDH: Gezond en Gelukkig Den Haag – dataonderzoeksproject Gezond en Gelukkig Den Haag.

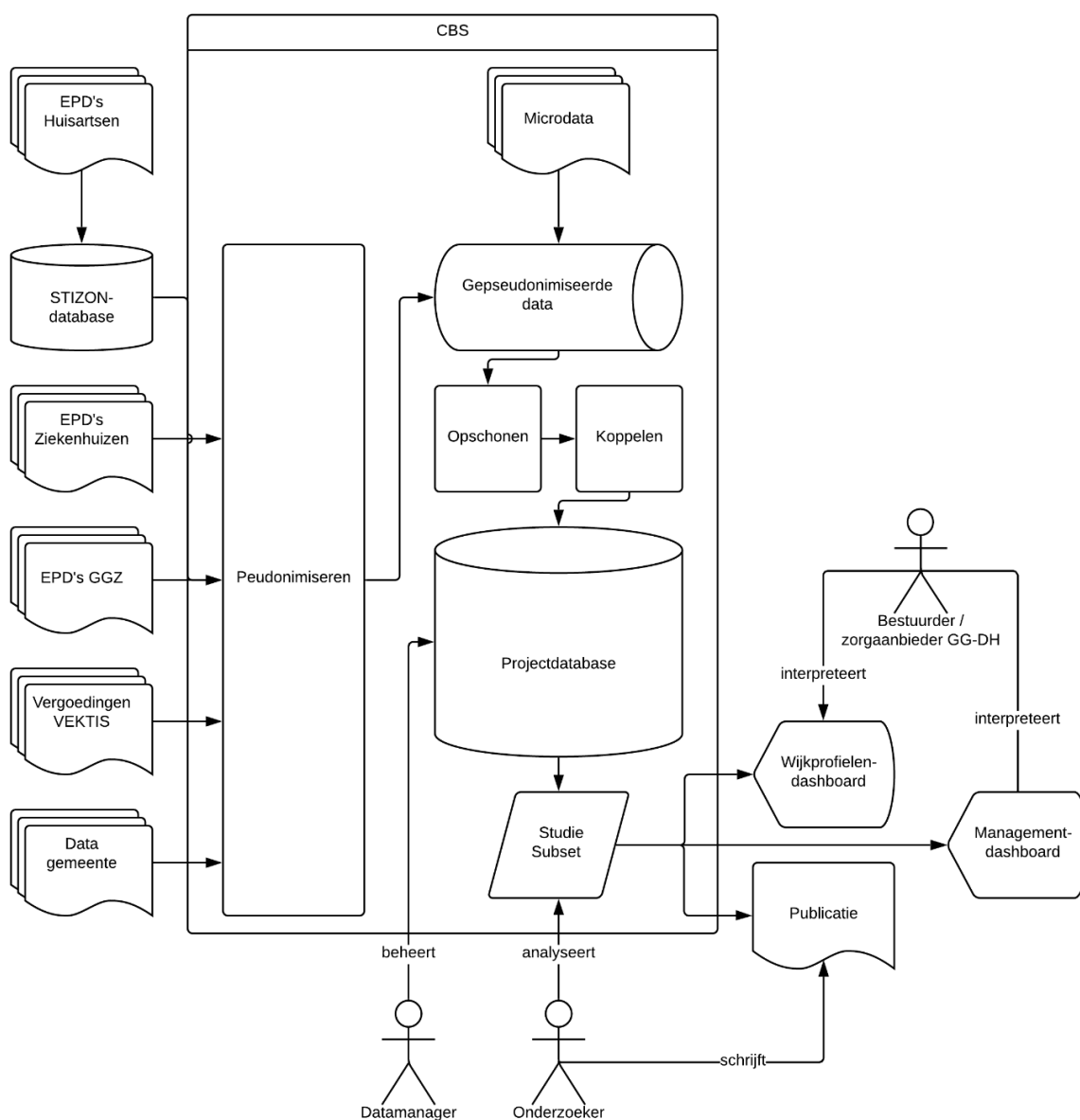
Kan aan de huisartsen worden teruggekoppeld om welke patiënten (dus niet geanonimiseerd) het gaat, zodat zij preventieve maatregelen kunnen treffen?

De laatste vraag is hierboven al aan bod gekomen. De informatie van de SEH kan gedeeld worden met de eigen huisarts, voorzover relevant voor de behandeling van de betrokkene. De eerste vraag is een onderzoeksvraag, waarvan duidelijk moet worden wat de doelstelling precies is. Gelet op de doelstelling kan deze vervat worden onder de daarvoor geldende structuur. Als het gaat om onderzoek en statistiek dan is het mogelijk deze kennis te vergaren volgens de regels voor wetenschappelijk onderzoek en statistiek. Dit gaat de door NVZ bepaalde scope van dit onderzoek te buiten.

Het lijkt niet te gaan om kwaliteitsonderzoek in dit geval, maar als dat anders is dan is de route onder onderzoeksvraag 1 beschreven aangewezen. De inzet van het Centraal Bureau voor de Statistiek (CBS) als vertrouwde derde partij (trusted third party) voor koppeling van data kan daarnaast ook overwogen worden, als gegevens noodzakelijk zijn voor een gerechtvaardigd doeleinde (zoals bijvoorbeeld wetenschappelijk onderzoek en statistiek). De methode en inrichting die gevolgd wordt in het ELAN- GGDH project is bestudeerd in dit onderzoek en is een goede methode. CBS heeft een wettelijke basis om dergelijke diensten te kunnen verlenen. Het is aan het CBS om aan te geven of zij behulpzaam kunnen zijn bij bepaalde dataverwerking.

Inzet CBS bij gegevensverwerking: Gezond en Gelukkig Den Haag

In het Data Governance document van ELAN-GGDH⁸ is een verwerkingsschema bijgevoegd:



⁸ LUMC Campus Den Haag, Data Governance, Dataonderzoeksproject ELAN Gezond en Gelukkig Den Haag

Een enkele opmerking ten aanzien van de inrichting betreft het verwerken van gegevens door de externe datamanager van het project binnen de omgeving van CBS.

In de beschrijving bij het plaatje wordt aangegeven dat de datamanager van het project degene is die zorgt voor opschonen en koppelen van data. Logischer zou zijn wanneer deze activiteit onder de verantwoordelijkheid van CBS gebeurt en de datamanager pas toegang krijgt tot de gegevens op projectdatabase niveau zoals in het plaatje wordt uitgebeeld. Wat betreft Stizon is niet precies duidelijk wat de juridische grondslag is om een één op één extract van het HIS te verwerken voor een huisarts. Deze verwerking ligt buiten de scope van het onderzoek. Voor dit onderzoek wordt de datastroom via Stizon verder als een gegeven beschouwd.

De route met het CBS als trusted partij voor koppeling van data kan altijd gevolgd worden, mits de gegevensverwerking noodzakelijk is voor het gerechtvaardigde doeleinde. CBS heeft een wettelijke basis om dergelijke diensten te verlenen, dus een en ander is afhankelijk van de wens van CBS om te ondersteunen.

Voorbeeld 2. *Opschaling / verbreding van teleconsultatie*

De huisarts legt een vraag voor aan specialist via online applicatie (TCCN) en krijgt antwoord terug in de vorm van gestandaardiseerd intercollegiaal advies.

Data issue (evaluatie): Is er toegang mogelijk tot de persoonlijke gegevens van patiënten die een teleconsult hebben gehad van huisartsen, om die te koppelen aan onze ziekenhuis data, om zo (geanonimiseerd) inzicht te krijgen in het percentage dat alsnog verwezen wordt.

De aanpak die in deze vraag wordt voorgesteld lijkt te moeten leiden tot een verwerking die veel ruimer is (meer gegevens bevat) dan nodig zou zijn, wanneer huisartsen zouden registreren welke patiënten zijn doorverwezen na consultatie, en de percentages zouden delen. Immers de gegevens zouden ook inhoudelijk bestudeerd moeten worden om te weten of een aangetroffen doorverwijzing van een persoon ook te maken heeft met het teleconsult. Percentages doorverwijzingen zouden op een andere wijze kenbaar kunnen worden naar verwachting. Als dit anders is en geoordeeld wordt dat dit noodzakelijk is voor de samenwerking en kwaliteit van de geleverde zorg, dan zou eventueel de route voor kwaliteitsdoel-einden gevolgd kunnen worden. Er is dan geen toegang mogelijk tot de patientendata van de huisarts, maar de huisarts zou gevraagd kunnen worden om gepseudonimiseerde data aan te leveren voor een vergelijking met de eigen gegevens, op basis van zo min mogelijk gegevens. (Zie boven onder onderzoeksvraag 1). Als het echter mogelijk is de gegevens op een voor de gegevensbescherming minder belastende manier te verkrijgen zoals hierboven gesuggereerd, dan wordt er niet voldaan aan de eis van noodzakelijkheid (subsidiariteit) om op deze wijze gegevens te verwerken. Een alternatief is de CBS route.

Voorbeeld 3. *Bij de keuzehulp kijken we o.a. naar het percentage reductie in operaties.*

Data issue (evaluatie): Om te kunnen monitoren of patiënten de operatie niet uitstellen maar afstellen is het van belang om inzicht te hebben in het huisartsdossier van patiënt. Hieruit kan dan worden opgemaakt of de patiënt niet elders een operatie heeft laten uitvoeren of dat een andere behandelmethode is gevolgd (bv. fysio).

Deze data zouden we op kunnen vragen bij de huisarts v/d patiënt maar uitwisseling van gegevens is nu nog niet aan de orde.

In dit voorbeeld gaat het eigenlijk om het op de hoogte blijven van de gang van de patiënt, nadat de behandelrelatie in het ziekenhuis is beëindigd. Er is wel een link met kwaliteit, maar niet per se of rechtstreeks. Er kunnen veel aspecten een rol spelen bij de keuze van de patiënt voor het vervolg (of niet) van zijn zorgtraject. De geheimhoudingsplicht en de vertrouwelijkheid maken dat deze gegevens niet gedeeld mogen worden zonder toestemming, of de toestemming verondersteld. De patiënt hoeft de verwerking ook niet te verwachten. Een patiëntenenquête kan wel inzicht geven in de keuzes van patiënten. Het is mogelijk om aan het gebruik van de keuzehulp (via de gegevens van de patiënt die bekend zijn om een inlog te genereren) een follow up te koppelen voor een bepaalde periode, waarbij patiënten worden uitgenodigd een enquête in te vullen na het voltooien van de keuzehulp. Een alternatief is nog om de patiënt als ziekenhuis zelf toestemming te vragen om de huisarts op een later moment te mogen vragen naar het vervolg van de behandeling, of de patiënt te vragen of deze gebeld mag worden daarover door een enquêteur van het ziekenhuis hiertoe. Beide methoden zijn iets complexer en het is de vraag of de noodzaak daartegen opweegt.

Voorbeeld 4. *Het project directe toegang radiodiagnostiek door Huisartsenpost (HAP) in de Avond Nacht Weekeinde (ANW) uren waardoor patiënt niet via chirurg op de Spoedeisende Hulp (SEH) een foto krijgt maar direct vanaf de HAP.*

Data issue (logistiek samenwerken): helaas moet de patiënt nog steeds worden ingeschreven op de SEH. Het inschrijven van de patiënt en het aanvragen van een X-ray is niet mogelijk door de HAP omdat zij niet in onze systemen kunnen en vice versa. Hierdoor worden onnodige administratieve processen /workarounds bedacht.

De aanleiding voor deze onmogelijkheid in de huidige werkwijze ligt niet op het terrein van de gegevensbescherming. Dat wil zeggen, een technische mogelijkheid om een X-ray aan te vragen door een externe zorgaanbieder (de HAP) zou juridisch mogelijk moeten zijn. Het is voor te stellen dat uit oogpunt van toegangsbeveiliging externe zorgaanbieders geen rechtstreekse toegang hebben tot het systeem van het ziekenhuis. Er staat echter niets aan in de weg om een technische oplossing te ontwikkelen om een aanvraag bij de radiologie door geselecteerde zorgaanbieders uit de regio (of verder) mogelijk te maken. Wellicht kan iets dergelijks via een berichtenstructuur worden ingericht of via een 'knop' op een platform of via een app. Waarschijnlijk kunnen bestaande structuren waarbinnen authenticatie al voorzien is ook uitkomst bieden hierbij, bijvoorbeeld Zorgdomein of het LSP van VZVZ.

Voorbeeld 5. *Wondzorg project: inzet van wondarts in de eerste lijn, om in samenwerking met thuiszorg en huisartsen eerstelijns zorg te versterken en te voorkomen dat patiënten naar tweedelijns wondcentrum moeten komen.*

Data issue (evaluatie): "het delen van data met de thuiszorg en huisartsen ter evaluatie van de pilot horizontaal doorverwijzen was best een lastige. Bij de thuiszorg was er een heel protocol hiervoor en moesten er overeenkomsten zijn. Formeel moest alles geanonimiseerd worden, wat veel tijd en werk kostte, maar dan zijn data veel lastiger te koppelen zodat dubbel tellingen voor komen (patiënt gezien door thuiszorg en huisarts voordat deze bij de wondpoli komt). Tevens is het traject dat een patiënt doorlopen heeft moeilijker te volgen als het anoniem gaat. Concreet betekent dat meer "vage" conclusies en aannames op basis van de data.

Het hangt er bij dit voorbeeld mede vanaf op welke wijze de wondarts wordt ingezet. Gaat deze namens de huisarts of de thuiszorg optreden in de eerste lijn? Of treedt hij op namens het ziekenhuis? Dat bepaalt ook wie het dossier voert. Voor te stellen is ook dat de wondarts in elk geval toegang houdt tot gegevens van patiënten die hij zelf gezien heeft in het dossier dat mogelijk bij de huisarts wordt gevoerd. Deze aspecten van de samenwerking maken allemaal uit. Het is logisch dat er een contractuele structuur is opgezet. Voor het evalueren van deze zorginhoudelijke samenwerking lijkt het in elk geval mogelijk om ook voor kwaliteitsdoeleinden de behandelde patiënten te monitoren, d.w.z. te weten of behandeling op de wondpoli daarna nog nodig is. De methode van aanpak zoals voor dit doeleinde van gegevensverwerking beschreven onder onderzoeksvraag 1 kan daarbij gehanteerd worden. Alternatief kan er ook gevraagd worden aan patiënten of zij eerder door de wondarts gezien zijn bij de huisarts of door de thuiszorg en of zij er in toestemmen die gegevens op te vragen. Misschien is deze vraag niet voor de hele populatie met uitsluiting te beantwoorden.

3.5 Service evaluation

Indien uit het onderzoek blijkt dat er sprake is van een juridisch probleem op het gebied van uitwisseling onder de genoemde doelstellingen, vind NVZ het interessant om te bestuderen of Service evaluation⁹ zoals in het Verenigd Koninkrijk ingezet, een mogelijkheid voor de Nederlandse omgeving is. In het VK maakt men juridisch onderscheid tussen wetenschappelijk onderzoek (met alle wettelijke eisen en voorwaarden) en de zogenoemde 'service evaluation'. Voor deze data analyse op populatie niveau zou volgens NVZ geen individuele toestemming nodig zijn.

Uit het onderzoek, gebaseerd op informatie van Engelse ziekenhuizen en de NHS, is gebleken dat er voor service evaluation geen aparte wettelijke regelingen zijn die aanvullen op de normale eisen aan gegevensverwerking in de zorg. In het VK is de Data Protection Act (2018) van toepassing (hun versie van de GDPR).

Er zijn daarnaast ethische normen (gedragcodes) ter bescherming van de privacy van patiënten die van toepassing zijn op alle soorten gezondheidsonderzoek, service evaluation en auditprocessen. Onderzoeksprojecten die in de gezondheidszorg worden uitgevoerd, hebben normaal gesproken goedkeuring nodig van een ethische commissie voor onderzoek of een Institutional Review Board (IRB), evenals van de zorginstelling(en) zelf.

Een service evaluation of audit vereist mogelijk geen specifieke goedkeuring van een ethische onderzoekscommissie of IRB, maar ethische principes moeten nog steeds worden nageleefd voor de bescherming van patiënten. In het Verenigd Koninkrijk is het uitgangspunt toestemming óf geen bezwaar op basis van informatie. Potentiële deelnemers worden geïnformeerd over deelname aan het project. Ze hebben het recht om deelname te weigeren en zich op elk moment terug te trekken.¹⁰

⁹ Service evaluation seeks to assess how well a service is achieving its intended aims. It is undertaken to benefit the people using a particular healthcare service and is designed and conducted with the sole purpose of defining or judging the current service. The results of service evaluations are mostly used to generate information that can be used to inform local decision-making.

¹⁰ The Healthcare Quality Improvement Partnership (HQIP) has a useful guide in relation to applying ethical principles to service evaluations and audits. This can be downloaded from: www.hqip.org.uk/assets/.../Audit-Research-Service-Evaluation.pdf

Concluderend uit deze bevindingen is er eigenlijk geen of weinig verschil met de Nederlandse situatie. Ook in Nederland is kwaliteitstoetsing en onderzoek mogelijk op basis van de wetgeving. In beginsel worden daartoe niet herleidbare gegevens gebruikt. Deze kunnen door een kwaliteitsmedewerker die aan bepaalde eisen voldoet uit het proces gehaald en bijvoorbeeld voor koppeling gepseudonimiseerd worden, en vervolgens geanonimiseerd/gecodeerd met een uniek volgnummer. Deze mogelijkheid sluit ook aan bij de kwaliteitstoetsing die vereist is op grond van artikel 7 Wkkgz en de ontheffingen van de AVG/UAVG zoals hierboven al aan de orde gekomen. In veel gevallen kan van veronderstelde toestemming worden uitgegaan voor de doorbreking van de geheimhouding om de gegevens te kunnen benaderen en verder verwerken. Waarbij gegevens dus zo snel als mogelijk daarna niet herleidbaar worden gemaakt. Dit sluit aan bij een 'geen bezwaar' regime dat in de UK soms van toepassing kan zijn.

3.6 Mogelijke andere routes

In de zorg zijn diverse dataverwerkers actief die vaak als trusted third party gegevens voor benchmark, onderzoek en analyse verwerken. Zij werken in opdracht van zorgaanbieders, zoals de ziekenhuizen.

Ook zijn er kwaliteitsregistraties zoals Dutch Hospital Data.

Alle ziekenhuizen hebben contracten met dataverwerkers die voor hen gegevens verwerken en terugleveren. Daarbij worden ook gegevens van andere zorgaanbieders gekoppeld. Zonder hier namen te noemen en daarmee een partij aan te bevelen of uitspraken te doen over de grondslag voor gegevensverwerking door deze verschillende partijen, kan het nuttig zijn voor ziekenhuizen om na te gaan óf en hoe zij gebruik kunnen maken van al bestaande structuren en gegevensregistraties in het kader van JuMP.

Derhalve kan het een optie zijn voor ziekenhuizen om die mogelijkheden te onderzoeken. PrivacyCare kan dit ook voor de ziekenhuizen nader onderzoeken.

4. Conclusies en aandachtspunten

4.1. Doeleinden voor verwerking

In hoofdstuk 3 is uiteengezet welke gegevensverwerkingen onder omstandigheden mogelijk zijn, onder welke voorwaarden. Samengevat zijn er een aantal opties met bepaalde uitgangspunten. Allereerst is het altijd belangrijk te bepalen wie voor welke doeleinden gegevens wil verwerken. Dit bepaalt of er een grondslag is in de wetgeving. Vervolgens mogen gelet op het doeleinde dat gerealiseerd wil worden, alleen de noodzakelijke gegevens verwerkt worden.



Relevante doeleinden in dit onderzoek zijn:

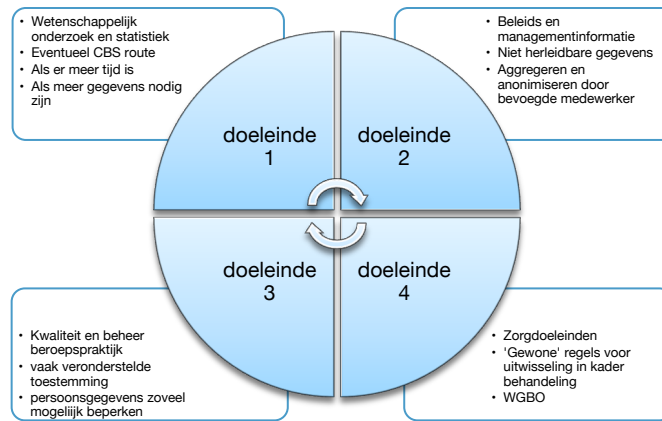
1. Wetenschappelijk onderzoek of statistiek
2. Beleids- en managementinformatie genereren
3. Kwaliteitsdoeleinden
4. Zorgdoeleinden/ zorgverlening

Voor doeleinde 1 geldt dat de regels voor wetenschappelijk onderzoek en statistiek gevolgd worden, inclusief relevante gedragscodes. Omdat deze regels op andere plekken zijn uitgewerkt valt dit buiten de scope van het onderzoek. In het onderzoek is wel het verwerken van gegevens via het CBS besproken, wat een goede methode is voor dit doeleinde, maar ook uitkomst kan bieden als de mogelijkheden voor gegevensverwerking voor de andere doeleinden vastlopen.

Voor doeleinde 2 is het uitgangspunt dat in beginsel geen herleidbare gegevens hoeven te worden verwerkt.

Voor doeleinde 3 geldt dat dit onder het beheer van de instelling en de beroepspraktijk valt en er een ontheffing kan zijn onder de AVG en UAVG. Daarnaast mag in veel gevallen worden uitgegaan van veronderstelde toestemming van de patiënt op grond van de WGBO voor noodzakelijke gegevensverwerking voor dit doeleinde. Herleidbaarheid van de gegevens wordt niettemin zo snel en zo veel mogelijk beperkt of voorkomen.

Voor zorgdoeleinden zijn er de ‘gebruikelijke’ mogelijkheden voor het verwerken en delen van patiëntgegevens zoals voor de behandeling noodzakelijk, en zoals in hoofdstuk 2 en 3 van het rapport beschreven.



4.2 Verwerkingsverantwoordelijke en verwerker

Bij elke verwerking is het relevant om te bepalen wat ieders rol is. Zeker bij een samenwerking is dat niet altijd meteen duidelijk. Op de verwerkingsverantwoordelijke rusten andere verplichtingen dan op de verwerker. De verwerkingsverantwoordelijke is degene die de verantwoording moet afleggen voor het hebben van een rechtmatige grondslag voor verwerking. Wanneer een dataverwerker wordt ingeschakeld is het van belang de verwerkersrol goed geregeld te hebben. Dat voorkomt problemen met zeggenschap over gegevens. Een zorgaanbieder zoals een ziekenhuis moet de zeggenschap over herleidbare patientengegevens nooit uit handen geven. Dit is alleen anders als dit in een specifiek geval met toestemming of op verzoek van de patient gebeurt, dan wel wettelijk verplicht is.

4.3 Grondslag en noodzakelijke verwerking

Voor rechtmatige verwerking is een grondslag nodig op grond van de AVG. Uitgangspunt is om steeds alleen de noodzakelijke gegevens te verwerken voor het doeleinde van de verwerking. In de AVG komt dit terug als het principe van data minimalisatie. Het is altijd van belang om de noodzaak van gegevensverwerking te beoordelen en te evalueren aan de hand van het doeleinde waarvoor de verwerkingsgrondslag aanwezig is.

Er is geen grond om alle denkbare verbanden te onderzoeken uit vertrouwelijke gezondheidsgegevens. Of het doeleinde nu kwaliteitsbeheer of wetenschappelijk onderzoek of statistiek is, alleen de noodzakelijke gegevens mogen worden verwerkt voor het doeleinde.

BSN

Het gebruik van het BSN in de administratie van de zorgaanbieder en bij het uitwisselen van gegevens tussen zorgaanbieders is voorgeschreven om ervoor te zorgen dat steeds de gegevens betreffende een persoon met betrekking tot die persoon worden gebruikt (en opgeslagen). Het BSN mag alleen verwerkt worden voor het doeleinde van uitvoeren van zorg.

Het verwerken van het BSN mag alleen op grond van de wet of de doeleinden daarin genoemd. Tussen zorgaanbieders wordt het BSN uitgewisseld in verband met de goede zorgverlening. Voor zover en zolang kwaliteitsborging voortvloeit uit of essentieel is voor het leveren van goede zorg, zou men kunnen redeneren dat de verwerking van het BSN geboden is. Wanneer is dat het geval en waar eindigt het? Om een veilig onderscheid te maken wordt geadviseerd om een splitsing te maken in kwaliteitsborging voor individuele zorgverlening en kwaliteitsbeheer voor een populatie. In het eerste geval is het gebruik van het BSN nog van belang om terug te kunnen gaan naar de patient. In het tweede geval gaat het vooral om uitkomsten van zorg en eventuele aanpassingen toepassen op de populatie al geheel.

Dan moet verwerking van het BSN achterwege blijven en zou (niet terug te herleiden) gepseudonimiseerde of geanonimiseerde verwerking aangewezen zijn.

Encryptie leidt er zelden of nooit toe dat persoonsgegevens niet meer als persoonsgegeven hoeven worden beschouwd. Dit is met de AVG strenger geworden dan onder de voorganger Wbp. Dit heeft te maken met de digitalisering en de mogelijkheden die er kunnen zijn om databestanden samen te voegen en alsnog, ergens ter wereld, tot herleiding te kunnen komen. Daarom is de AVG van toepassing op gepseudonimiseerde BSN's

Vervolgens kan men zich afvragen of het ook gaat om het verwerken van het BSN als zodanig op de plek waar dit geëncrypt gebeurt. Op voorwaarde dat de encryptie zodanig sterk is dat het gegeven op deze plaatsen niet als BSN kan worden uitgelezen of ontcijferd, ook niet met behulp van anderen (technisch en organisatorisch uitgesloten) én passende beveiliging is doorgevoerd, kan beredeneerd worden dat geen sprake is van het verwerken van het BSN als zodanig op deze plaatsen (in verband met de BSN wetgeving).

4.4 Beveiliging van gegevens

De AVG vereist naast een adequate en passende gegevensbeveiliging tegen verlies van of andere inbreuk op gegevens dat privacy by default en design en dataminimalisatie worden toegepast. Zowel de verwerkingsverantwoordelijke(n) als door hen ingeschakelde verwerkers kunnen hierop zelfstandig worden aangesproken.

Passende gegevensbeveiliging moet altijd aantoonbaar worden gemaakt. De rechtmatigheid van verwerkingen in deze rapportage beschreven is altijd mede afhankelijk van het voldoen aan deze vereisten van de AVG. Het gaat dus niet uitsluitend om een wettelijke grondslag, maar ook om het voldoen aan de vereiste waarborgen voor extractie, veiligheid van uitwisseling en opslaan van gegevens. Waar worden gegevens bewaard? Hoe lang worden ze bewaard? Wie heeft toegang tot gegevens? Hoe wordt dat gecontroleerd? Het zijn allemaal vragen die de rechtmatigheid mede bepalen. En ook juridische afspraken (overeenkomsten) over de verwerking van de gegevens moeten in orde zijn.

Daarnaast is het zo dat authenticatie bij toegang tot gegevens moet gebeuren op een passend betrouwbaarheidsniveau. Dit is afhankelijk van de gegevens die worden ontsloten. Bij gegevens die onder het medisch beroepsgeheim vallen en het BSN is dat niveau "hoog".

4.5 Privacybeleid en rechten betrokkenen

Van belang is dat er een privacybeleid is opgesteld dat de processen en maatregelen binnen de organisatie van de verantwoordelijke borgt. Dit wordt door de AVG verlangd, in tegenstelling tot ad hoc beleid. Daarin moet ook worden geborgd hoe de rechten van betrokkenen worden nageleefd en waar betrokkene terecht kunnen voor informatie en met vragen of klachten. Afgesproken moet worden hoe betrokkenen worden geïnformeerd, op een bezwaarmogelijkheid worden gewezen, of in voorkomende gevallen om toestemming wordt gevraagd. Het is van belang om hierover in de instelling of met de samenwerkingspartners (afhankelijk van de verwerking) tot afspraken te komen en de verantwoordelijkheden te adresseren in het beleid.

De Algemene verordening gegevensbescherming gaat ook uit van een zogenaamde 'policy-based' naleving van de privacywetgeving. Daarbij is de 'accountability' van de verantwoorde-

lijke en de verwerker een beschreven uitgangspunt geworden. Vastgesteld en geïmplementeerd privacybeleid is daarbij een startpunt om aan te tonen dat de organisatie weet wat hij doet en waarom.

Ook is het in dit kader van belang een goede procedure te hebben vastgelegd en geïmplementeerd voor de afhandeling van zogenoemde 'datalekken' en de afspraken daarover tussen verantwoordelijke(n) en verwerker(s). Een verwerker is daarbij verplicht om een logboek bij te houden van alle 'datalekken' die zich voordoen ten behoeve van de verantwoordelijke en diens verantwoordingsplicht.

4.6 Geheimhouding

Met interne of externe medewerkers die toegang hebben tot persoonsgegevens moet altijd een geheimhoudingsverklaring of overeenkomst getekend worden. Dit kan in de arbeidsovereenkomst voldoende zijn omschreven. Geadviseerd wordt om na te gaan of voor eventuele medewerkers die betrokken zullen zijn bij de gegevensverwerking deze geheimhouding al expliciet geregeld is. Als er verwerkers zijn waarmee wordt samengewerkt dan zullen daarmee ook afspraken moeten worden gemaakt over vertrouwelijkheid en geheimhouding.

4.7 Slotconclusie

Patiëntgegevens zijn naar hun aard vertrouwelijk en mogen buiten de behandelrelatie niet zomaar gedeeld worden. Toch blijkt uit het onderzoek dat er een aantal goede mogelijkheden is om met gegevensverwerking de juiste zorg op de juiste plaats te bevorderen.

Vanuit een klankbordgroep zijn diverse casus aangereikt vanuit de zorg met de vraag “mogen we deze gegevens verzamelen om doel ‘x’ te bereiken?”

Voor veel van de gewenste gegevensverwerkingen bestaat een verwerkingsgrondslag. Bij elke beoogde gegevensverwerking moet bepaald worden welk doeleinde daarmee verwezenlijkt wordt. Wie, voor welk doeleinde, welke gegevens wil verwerken bepaalt of er in de wet een grondslag voor is en welke voorwaarden en beperkingen daarbij gelden.

Als er een grondslag is mag slechts de noodzakelijke gegevensverwerking plaatsvinden. Wat is de meest geëigende manier van verwerken om het doeleinde te verwezenlijken? Vanuit het vereiste van dataminimalisatie (en privacy by design) is van belang om op de juiste plaats gegevens te verzamelen of verwerken. Wie in de keten kan het beste (onder de juiste verantwoordelijkheid en met de minste uitwisseling van gegevens) een vraag beantwoorden? Daar zou -in beginsel- de verwerking moeten plaatsvinden.

Wanneer gegevensverwerking niet voor kwaliteitsdoeleinden mogelijk is kan een verwerking op grond van wetenschappelijk onderzoek of statistiek nog uitkomst bieden. Service evaluation is niet nodig in Nederland, verwerking voor kwaliteitsdoeleinden levert dezelfde mogelijkheden. Het CBS en ook andere dataverwerkers kunnen eventueel uitkomst bieden. Bij CBS is de veiligheid op grond van de CBS wetgeving goed gewaarborgd en partijen zijn hierbij afhankelijk van welke vraag het CBS wil ondersteunen. Daarvoor is afstemming met CBS van belang.

Bijlage 1 Uitwerking Toetsingskader

1.1 Wet op de geneeskundige behandelingsovereenkomst

De WGBO is van toepassing op het verwerken van gegevens door de zorgverlener die hij in het kader van de behandeling van de patiënt heeft verkregen. Die wet verplicht hem de noodzakelijke gegevens vast te leggen in zijn dossier over de patiënt. Wanneer de zorgverlener gegevens over de patiënt wil delen heeft hij te maken met het medisch beroepsgeheim dat in de WGBO verankerd is.¹¹ Aan de patiënt zelf worden gegevens op diens verzoek verstrekt.

Ook als een verstrekking op grond van de AVG of Uitvoeringswet AVG geoorloofd is, kan het medisch beroepsgeheim toch aan die uitwisseling in de weg staan. Om de legitimiteit van een gegevensverstrekking te toetsen is daarom in de eerste plaats een toetsing aan de regels van het medisch beroepsgeheim nodig.

In de WGBO (artikel 7:457 en 7:458 BW) wordt geregeld in welke gevallen gegevens van de patiënt met anderen mogen worden gedeeld, en wanneer daarvoor toestemming nodig is. Artikel 7:458 BW gaat over de verstrekking van gegevens voor wetenschappelijk onderzoek.

Artikel 7:457 BW

Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.

Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.

Daaronder zijn evenmin begrepen degenen wier toestemming ter zake van de uitvoering van de behandelingsovereenkomst op grond van de artikelen 450 en 465 is vereist. Indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.

‘Hulpverlener’ in de WGBO is volgens de memorie van toelichting zowel de individuele hulpverlener (de behandelaar/dossiervoerder) als de zorgaanbieder voor wie of waarvoor hij werkt. Beiden hebben een verantwoordelijkheid voor het waarborgen van het beroepsgeheim en dus een gedeelde verplichting om in een rechtsgeldige toestemming te voorzien. Uit artikel 7:457 BW volgt dat hulpverleners gegevens over patiënten aan anderen mogen verstrekken als dat wettelijk verplicht is, als die anderen rechtstreeks betrokken zijn bij de

¹¹ Het medisch beroepsgeheim vloeit voor zorgverleners ook voort uit artikel 88 Wet BIG. In de WGBO is het beroepsgeheim in verband met de behandelingsovereenkomst nader uitgewerkt.

uitvoering van de behandelingsovereenkomst of vervanger zijn van de hulpverlener. Verstrekken van gegevens mag ook aan de vertegenwoordiger van de patiënt, of als de patiënt daarvoor toestemming heeft gegeven.

Rechtsgeldige toestemming ontheft de hulpverlener van zijn zwijgplicht en geeft de hulpverlener een spreekrecht. De hulpverlener heeft geen spreekplicht of kan niet gedwongen worden het geheim te doorbreken. Hij is zelf verantwoordelijk voor het maken van een professionele afweging waar hij dat nodig acht. Met het verlenen van toestemming aan een hulpverlener (of zorgaanbieder) om gegevens uit diens medisch dossier met andere zorgaanbieders te delen, geeft de patiënt dus tevens toestemming aan de hulpverlener om diens beroepsgeheim te mogen doorbreken.

Veronderstelde toestemming

Om het beroepsgeheim te mogen doorbreken, mag de toestemming van de patiënt soms worden verondersteld. Bijvoorbeeld als een patiënt bij een actuele hulpvraag wordt doorverwezen naar een andere hulpverlener die de behandeling overneemt, of bij een gegevensverstrekking voor secundaire doelen, zoals het beheer van dossiers, de financiële afwikkeling, opleiding, kwaliteitsbewaking en kwaliteitsbevordering. Ook een medisch specialist die de huisarts van zijn patiënt wil informeren, mag daarvoor de toestemming veronderstellen. Maar patiënten moeten wel de mogelijkheid hebben om bezwaar te maken daartegen. Daarom moeten zij vooraf zijn geïnformeerd over de mogelijke gegevensverstrekking en over de bezwaarmogelijkheid.

In de KNMG-richtlijn “Omgaan met medische gegevens” worden twee situaties onderscheiden waarin de toestemming van de patiënt mag worden verondersteld. In de eerste situatie is de patiënt op de hoogte van de gegevensverstrekking. Deze situatie doet zich bijvoorbeeld voor bij een verwijzing van de patiënt door een huisarts naar een medisch specialist. Als de patiënt instemt met de verwijzing, mag worden verondersteld dat hij ook instemt met het verstrekken van informatie aan die medisch specialist. De patiënt mag wel bezwaar maken tegen het verstrekken van alle of bepaalde gegevens, waarna de toestemming daarvoor uiteraard niet langer kan worden verondersteld.

In de tweede situatie is de patiënt niet op de hoogte van de gegevensverstrekking. Deze situatie kan zich voordoen als een patiënt niet of niet meer in staat is om toestemming te geven voor de gegevensverstrekking. De toestemming moet dan kunnen worden afgeleid aan de hand van aanwijzingen of gedragingen uit het verleden. Op grond daarvan kunnen bepaalde gegevens op grond van veronderstelde toestemming worden verstrekt aan een partner of familie van de patiënt, bijvoorbeeld als die partner telkens aanwezig was tijdens de bezoeken aan de arts. De veronderstelling van toestemming eindigt ook hier zodra de patiënt bezwaar maakt tegen de gegevensverstrekking.

De toestemming van de patiënt voor het verlenen van toegang tot bepaalde patiëntengegevens kan dus op grond van de WGBO worden verondersteld:

- in concrete situaties (inclusief spoedeisende zorg);
- waarin het kenbaar is voor de patiënt dat:
 - gegevens voor zorgdoeleinden worden verstrekt (inclusief overdracht van zorg, zorgondersteuning zoals dossierbeheer, financiële afwikkeling en dergelijke);
 - de patiënt daartegen geen bezwaar heeft gemaakt; en

- de gegevensverstrekking beperkt blijft tot hetgeen noodzakelijk is voor de ontvanger.

Dit laat onverlet dat op basis van andere wetgeving aanvullende eisen kunnen gelden, zoals in de situatie dat de Wabvpz van toepassing is (zie hieronder).

1.2 De Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG

De AVG is per 25 mei 2018 in werking getreden. Het is de belangrijkste wetgeving op het gebied van de bescherming van persoonsgegevens in de EU. De verordening geldt rechtstreeks in Nederland. Naast de AVG is er de Uitvoeringswet AVG (UAVG).

Er wordt een accent gelegd op accountability in de AVG. Dat betekent dat organisaties die persoonsgegevens verwerken, verplicht worden hun verwerkingsprocessen te beschrijven en zodanig in te richten dat ze steeds in staat zijn aan te tonen dat ze voldoen aan de wet. Naast het algemene vereiste dat iedere organisatie moet zorgdragen voor een adequate beveiliging verplicht de AVG organisaties om voor sommige hoog risico verwerkingen “privacy impact assessments” (PIA) te verrichten, en in zijn algemeenheid om “privacy by design” toe te passen en privacy by default in te richten en dit alles vast te leggen.

Onder de AVG moeten organisaties aandacht besteden aan de wijze van informeren van betrokkenen over de verwerking van hun persoonsgegevens. Ook om te voldoen aan het inzage- en correctierecht en 'wissingsrecht' zal een organisatie processen moeten inrichten.

Enkele relevante bepalingen

Hieronder zijn enkele bepalingen opgenomen die relevant zijn voor het onderzoek en het begrip van de AVG.

Verwerkingsverantwoordelijke en verwerker

De normen van de AVG richten zich grotendeels tot de ‘verwerkingsverantwoordelijke’ voor de gegevensverwerking. Dit is volgens de AVG ‘degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt’. Wanneer een zelfstandige partij de gegevens verwerkt in opdracht en voor doelstellingen van de verwerkingsverantwoordelijke treedt zij op als ‘verwerker’ van de gegevens in de zin van de AVG. De verwerker handelt onder eigen gezag. Dit is bijvoorbeeld aan de orde bij hosting van een database door een derde dienstverlener, het in gebruik geven van een server en SAAS.

Zorgaanbieders zijn verwerkingsverantwoordelijke voor de gegevens van patiënten die zij behandelen. Dat kunnen instellingen zoals ziekenhuizen zijn, maar ook de individuele zorgverlener zoals de huisarts.

Artikel 5 Beginselen inzake verwerking van persoonsgegevens

Persoonsgegevens moeten:

- a. worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;
- b. voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeen-

komstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd;

c. toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;

d. juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren;

e. 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; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen;

f. door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en moet naleving aantonen.

Bewaren van gegevens

Persoonsgegevens mogen slechts worden verwerkt als zij voor het specifieke doeleinde van verwerken noodzakelijk zijn en niet langer worden bewaard dan noodzakelijk.

Grondslag

De AVG vereist een grondslag voor de gegevensverwerking op grond van artikel 6 lid 1 AVG. Daarin wordt aangegeven voor welke doeleinden persoonsgegevens verwerkt mogen worden.

Artikel 6 Rechtmatigheid van de verwerking

1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

- a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van

een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

(...)

Toestemming

Artikel 7 regelt de voorwaarden van toestemming. Als toestemming de grondslag is, moet de verantwoordelijke kunnen aantonen dat geldige toestemming is gekregen. En dat het voor mensen net zo makkelijk is om hun toestemming in te trekken.

Artikel 4 geeft de definitie van toestemming:

elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

De toestemming dient te zijn gegeven op basis van adequate, juiste en volledige informatie. De informatie mag zowel mondeling als schriftelijk of digitaal gegeven zijn, maar de zorgaanbieder wordt geadviseerd om schriftelijke (digitale) informatie te verstrekken en beschikbaar te hebben voor latere raadpleging, in verband met de aantoonbaarheid.

Overwegingen 42 en 43 van de AVG zijn hier relevant. Daarin wordt onder andere uitgelegd dat de verwerkingsverantwoordelijke (hier de zorgaanbieder) toestemmingsinformatie moet verstrekken in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. Toestemming is niet vrijelijk verleend, en dus ongeldig, als de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

De toestemming wordt ook geacht niet vrijelijk te zijn verleend als geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is. Ook mag het verlenen van zorg niet afhankelijk worden gemaakt van de toestemming.

Artikel 9 Verwerking van bijzondere categorieën van persoonsgegevens

1. Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

2. Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:

a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of

lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven.

(...)

h) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorg stelsels en diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

(...)

i) de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim;

Bij zorgverlening is de ontheffing van lid 2 sub h steeds voldoende. Wanneer er sprake is van toestemming voor het verstrekken of verwerken van persoonsgegevens dan correspondeert dat met de ontheffing zoals bedoeld wordt in artikel 9.2.a AVG.

Ook de UAVG regelt uitzonderingen op het verbod van artikel 9 AVG (zie hieronder).

BSN verwerking

Een nummer dat bij wet is voorgeschreven om een persoon te identificeren, mag alleen mag worden gebruikt voor de uitvoering van die wet. Of voor doeleinden die in de wet staan. Dat staat in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Dit is een uitwerking van artikel 87 AVG.

Het BSN is zo'n identificatienummer. Organisaties kunnen het verbod om het BSN te gebruiken niet doorbreken door toestemming aan mensen te vragen voor het gebruik van hun BSN.

Regels over het verwerken van het BSN zijn vervat in de Wet algemene bepalingen burgerservicenummer (Wabb) en in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Voor zorgaanbieders is het verwerken van het BSN verplicht in hun administratie en bij uitwisseling met andere zorgaanbieders en verzekeraars.

Beveiligingseisen

Op grond van de AVG (artikel 32) dienen de verantwoordelijke en verwerker passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. 'Passend' betekent in dit verband dat de beveiliging in overeenstemming is met het risico van de gegevensverwerking (in verband met onder andere de aard van de gegevens en het gebruik) en de stand van de techniek.

Artikel 32 Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

- a) de pseudonimisering en versleuteling van persoonsgegevens;
- b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij beoordeling van een passend beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

(...)

Artikel 25 AVG vereist privacy by design en privacy by default. Deze eisen zorgen voor maximale dataveiligheid, zo min mogelijk onnodige herleidbaarheid en dataminimalisatie.

Artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

In de zorg is de NEN 7510 normering van belang voor goede toepassing van beveiligingsstandaarden. Daarnaast zijn er andere beveiligingsstandaarden relevant zoals de ISO/IEC 27000 (serie) standaarden.

Inschakelen verwerker

Artikel 28 regelt onder andere dat wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, de verwerkingsverantwoordelijke uitsluitend een beroep doet op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. De verplichting om een verwerkersovereenkomst te sluiten volgt uit artikel 28 lid 3 AVG. In de verwerkersovereenkomst moet tenminste aan de orde komen op grond van die bepaling dat verwerker:

- a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
- b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;
- d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
- e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;
- f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;
- g) na afloop van de verwerkdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
- h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

Meldplicht datalekken

Ook moet onder de AVG rekening gehouden worden met de meldplicht datalekken.

De AVG stelt in artikel 33 eisen aan de eigen registratie van de datalekken die zich in de organisatie hebben voorgedaan. De verantwoordelijke/verwerker moeten alle datalekken documenteren. Met deze documentatie kan de AP controleren of aan de meldplicht is voldaan. Van belang is om dit ook in de verwerkersovereenkomsten die gesloten gaworden op te nemen.

Uitvoeren Gegevenseffectbeoordeling

De verplichting om een gegevenseffectbeoordeling of DPIA uit te voeren in bepaalde gevallen (artikel 35 AVG) rust op de verantwoordelijke. Verantwoordelijke en verwerker werken samen om tot een goede DPIA te komen. De verwerker kan de PIA ook namens de verantwoordelijke of zelfstandig een PIA uitvoeren. De AVG stelt criteria voor het moeten uitvoeren van een DPIA. Een DPIA is onder andere vereist wanneer grootschalige verwerking van bijzondere gegevens aan de orde komt. De AP en de Europese toezichthouders hebben soorten verwerkingen benoemd welke in elk geval onder de verplichting vallen.

Artikel 35 Gegevensbeschermingseffectbeoordeling

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

(...)

Rechten betrokkenen

Hoofdstuk III van de AVG regelt de rechten van betrokkenen. Bij verwerking met behulp van een verwerker dient verwerker de verantwoordelijke te ondersteunen in de naleving van deze rechten.

(...)

Artikel 13 Informatieplicht

AVG regelt dat naast informeren over de gegevensverwerking, verwerkingsverantwoordelijke, de doeleinden, de grondslag, de ontvangers van de gegevens en de rechten van betrokkenen, ook geïnformeerd moet worden over:

- dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of
- de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;

Register van de verwerkingsactiviteiten

Overeenkomstig artikel 30 AVG houdt elke verwerkingsverantwoordelijke (en zijn vertegenwoordiger) een register bij van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden.

Ook de verwerker (en zijn vertegenwoordiger) houdt een register bij van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht.

1.3 De Uitvoeringswet AVG (UAVG)

De Uitvoeringswet AVG bevat, als uitwerking van artikel 9 AVG ontheffingen voor het verbod op het verwerken van gezondheidsgegevens.

Artikel 22.2 Uitvoeringswet AVG is een uitwerking van art. 9.2.a AVG en luidt, voor zover hier relevant, als volgt:

Overeenkomstig artikel 9, tweede lid, onderdelen a, c, d, e en f, van de verordening is het verbod om bijzondere categorieën van persoonsgegevens te verwerken niet van toepassing, indien:

- a. de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden;
- b. de verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon, indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

Vitale belangen

Voor situaties waarbij sprake is van vitaal belang van de betrokkene (levensbedreigende situaties) en de persoon niet in staat is toestemming te geven is er een extra ontheffing in artikel 9 lid 2 sub c AVG en artikel 22.2.b UAVG. Deze ontheffing is algemeen van aard en geldt voor alle soorten gegevensverwerking, niet alleen gezondheidsgegevens. Deze ontheffing kan ter beoordeling van een zorgaanbieder ingezet worden. Deze ontheffing is bruikbaar om bij andere zorgaanbieders informatie over de patiënt op te vragen. Als een patiënt eerder geen toestemming heeft gegeven om zijn gegevens in een elektronisch uitwisselingssysteem te zetten, zijn deze gegevens ook in een noodsituatie niet beschikbaar. Voor pushverkeer van gegevens is de ontheffing dan wel in te zetten.

Zorgverlening

Artikel 30.3 Uitvoeringswet AVG luidt, voor zover hier relevant, als volgt:

Gelet op artikel 9, tweede lid, onderdeel h, van de verordening, is het verbod om gegevens over gezondheid te verwerken niet van toepassing indien de verwerking geschiedt door:

- a. hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, voor zover de verwerking noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk;

Kwaliteitsbeheer

Het begrip 'beheer' dient in dit onderdeel te worden uitgelegd als het waarborgen van de kwaliteit van de verleende zorg, intercollegiale toetsing door hulpverleners onderling (kwaliteitsbeheer) en de betaling van rekeningen voor medische behandeling.

Op grond van artikel 30.3.a Uitvoeringswet AVG is deze ontheffing voldoende om persoonsgegevens van patiënten te verwerken. Daarvoor is geen toestemming als bedoeld in artikel 9.2.a (of artikel 22 Uitvoeringswet AVG) vereist.

Wat de grondslag uit de UAVG of AVG ook is, voor verstrekken van persoonsgegevens van patiënten is in alle gevallen tevens een grondslag voor het doorbreken van het beroepsgeheim nodig.

1.4 Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

De Wabvpz reguleert elektronische gegevensuitwisseling nader. De belangrijkste bepalingen in de Wabvpz zijn het recht van de patiënt om uitdrukkelijke toestemming te verlenen voor uitwisseling via een uitwisselingssysteem en de verplichting voor zorgaanbieders om elektronische inzage te verlenen aan patiënten.

artikel 15a - Toestemming voor uitwisseling via uitwisselingssysteem

De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselings systeem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven.

Artikel 15a, lid 2 Wabvpz dat beoogde gespecificeerde toestemming te regelen, treedt niet in werking. Toestemming dient niettemin te voldoen aan de eisen van artikel 7 AVG, en is altijd specifiek.

Om de bepalingen uit de Wabvpz goed te interpreteren is de definitie van elektronisch uitwisselingssysteem bepalend. De wet definieert een elektronisch uitwisselingssysteem als: “een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier”.

Omdat ‘raadpleegbaar’ kunnen maken ruimte laat voor interpretatie is het doel van de wetgever hier belangrijk. Voor de toepassing van dit artikel heeft de wetgever gedacht aan ‘pull-verkeer’ van gegevens. Dit blijkt uit de wetstoelichting en uit de Factsheet die de minister heeft opgesteld. Pull-verkeer is dan: het beschikbaar stellen van gegevens in een dossier van een zorgaanbieder voor (latere) raadpleging (voor een bepaald doel) door andere zorgaanbieders, zonder dat op het moment van het verlenen van toestemming bekend is wie die andere zorgaanbieders zullen zijn.

Het is nadrukkelijk de bedoeling van de wetgever geweest om de WGBO-uitzonderingssituaties voor het vragen van toestemming te laten bestaan. Het waarnemen voor elkaar in elkaars praktijk kan zonder de uitdrukkelijke toestemming wanneer geen ‘elektronisch uitwisselingssysteem’ wordt gebruikt. Voor het sturen van een elektronisch push-bericht bij vervanging of medebehandeling is ook geen uitdrukkelijke toestemming vooraf nodig.

Artikel 15a Wabvpz richt zich tot de zorgaanbieder die de gegevens beschikbaar maakt voor elektronisch raadpleging. De Wabvpz bevat nadere regels ten opzichte van de AVG en de WGBO en gaat specifiek in op het gebruik van elektronische uitwisselingssystemen.

Na de implementatie van de Wabvpz zal verder duidelijk moeten worden wat onder een uitwisselingssysteem moet worden verstaan omdat er situaties zullen zijn waarin het de vraag is of het om een uitwisselingssysteem gaat. Omdat de definitie bepaalt dat een dossiersysteem binnen een zorgaanbieder niet als uitwisselingssysteem kwalificeert, is het voor uitvoering mede relevant wanneer er sprake is van een zorgaanbieder.

Vragen die kunnen ontstaan zijn:

- Wat als er sprake is van een systeem dat wordt gebruikt voor uitwisseling van patientgegevens tussen zorgaanbieders, maar de gegevens daarmee (op basis van een WGBO

grondslag) in een pushbericht naar de ontvanger worden gestuurd?

- Wat als meerdere zelfstandige zorgaanbieders ook gezamenlijk een zorgaanbieder vormen (bijvoorbeeld als zorggroep) en uitwisseling met elkaar via een informatiesysteem mogelijk maken in het kader van bijvoorbeeld ketenzorg?

De wetgever heeft de eerste situatie niet bedoeld onder het toepassingsbereik te laten vallen; op systemen voor push-verkeer gelden de regels van de WGBO en AVG en is geen gespecificeerde toestemming op basis van de Wabvpz nodig. Gegevens worden namelijk niet raadpleegbaar gemaakt voor andere zorgaanbieders maar slechts aan een gerichte ontvanger gestuurd. Het gaat niet om pull maar om push van gegevens naar een ontvanger.

In de tweede situatie gaat het feitelijk om uitwisseling tussen verschillende zorgaanbieders uit en met eigen dossiersystemen die door koppeling bevraagd kunnen worden. Er is geen sprake van gerichte push, maar van inzien door aangesloten zorgaanbieders (ongericht). De Wabvpz is daarom van toepassing; een patiënt moet voor het gebruik van een dergelijk systeem gespecificeerde toestemming geven.¹²

Het derde lid van artikel 15a Wabvpz stelt dat het beschikbaar stellen onder deze voorwaarden is toegestaan voor zover de persoonlijke levenssfeer van een ander dan de cliënt niet wordt geschaad. Hiermee wordt bedoeld op gegevens van familieleden en andere betrokkenen die in het dossier kunnen zijn opgenomen.

artikel 15c Wabvpz - Informeren en registreren

De zorgaanbieder geeft de cliënt informatie over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen en over de werking van het elektronisch uitwisselingssysteem dat voor de gegevensuitwisseling wordt gebruikt. Indien nieuwe categorieën van zorgaanbieders aansluiten bij het elektronisch uitwisselingssysteem, of de werking van het elektronisch uitwisselingssysteem anderszins substantieel wordt gewijzigd, informeert de zorgaanbieder de cliënt over deze wijziging alsmede over de mogelijkheid om de gegeven toestemming, bedoeld in artikel 15a, aan te passen of in te trekken.

De zorgaanbieder houdt een registratie bij van de door cliënten verleende toestemming waarbij wordt aangetekend vanaf welk tijdstip de toestemming van kracht is geworden. De zorgaanbieder mag deze registratie beschikbaar stellen via het uitwisselingssysteem.

Wijzigingen in de gegevensverwerking waarvoor toestemming gegeven is

De tweede volzin van artikel 15c lid 1 Wabvpz legt de Factsheet van de minister als volgt uit: Het informeren over het aansluiten van nieuwe categorieën zorgaanbieders op een elektronisch uitwisselingssysteem is een eis, maar de uitwisseling van gegevens kan pas voor de uitbreiding aan de orde zijn als de toestemming voor die uitbreiding door de patiënt is aangepast (voor die nieuwe categorie had de patiënt immers nog geen gespecificeerde toestemming gegeven). Bij niet substantiële wijzigingen kan volstaan worden met alleen aanvullend informeren. Het is aannemelijk dat een te ruime interpretatie van wat 'niet substantieel' is in strijd kan worden geacht met de (Europese) grondrechten. Toestemming heeft im-

¹² Juridisch kennisdocument Toestemming, Programma GTS 2018, auteurs Nouwt & Krabben

mers de reikwijdte van de vooraf gegeven informatie. De Nederlandse wetgeving kan geen afwijking creëren die daarmee strijdig zou worden.

Wat is nu substantieel? Uit het gebruik van de term ‘anderszins’ kan worden afgeleid dat het aansluiten van nieuwe categorieën zorgaanbieders een substantiële wijziging is. Mede gelet op de Factsheet van de minister en de wetstoelichting is aannemelijk dat het bij substantiële wijzigingen i.e.g. moet gaan om aanpassingen van de doeleinden van gegevensverwerking, van een uitbreiding van gegevenssoorten, van een uitbreiding van categorieën ontvangers of bijvoorbeeld een wijziging van de verantwoordelijke voor de gegevensverwerking.

1.5 Wet Publieke Gezondheid (WPG)

Gevraagd is te onderzoeken welke grondslagen de WPG biedt voor uitwisselingen waar in het onderzoek naar gekeken wordt. De WPG regelt de publieke gezondheidszorg. Dit wordt gevormd door de gezondheidsbeschermende en gezondheidsbevorderende maatregelen voor de bevolking of specifieke groepen daaruit, waaronder begrepen het voorkómen en het vroegtijdig opsporen van ziekten. Jeugdgezondheidszorg en Ouderengezondheidszorg zijn specifieke onderdelen daarvan. De wet legt de organisatie van de publieke gezondheidszorg bij de gemeenten, met uitzondering van de specifieke verantwoordelijkheid en taken van de minister en het RIVM. Het college van burgemeester en wethouders bevordert de totstandkoming en de continuïteit van en de samenhang binnen de publieke gezondheidszorg en de afstemming ervan met de curatieve gezondheidszorg en de geneeskundige hulpverlening bij ongevallen en rampen. Het college draagt bij aan opzet, uitvoering en afstemming van preventieprogramma's, met inbegrip van programma's voor de gezondheidsbevordering. Er zijn dus een aantal taken die raken aan de intenties van het programma JuMP, echter op een beperkt gebied. Bij ouderengezondheidszorg zou een preventief programma of een gezondheidsbevorderend programma kunnen aansluiten bij de JuMP doelstellingen van ziekenhuizen. Dat betekent dat de instanties die in opdracht van de gemeente zorg dragen voor uitvoering van WPG elementen, zoals de GGD'en en ouderenzorgorganisaties, interactie nodig hebben met de curatieve gezondheidszorg, zoals de ziekenhuizen en huisartsen. Op grond van artikel 2 van de WPG kunnen zorgaanbieders ook verplicht worden gesteld gegevens te delen met het college of de GGD'en of ouderenzorgorganisaties, maar het gaat in dit geval om niet tot de patiënt herleidbare gegevens.

Het college van B en W draagt zorg voor de uitvoering van de jeugdgezondheidszorg en de ouderengezondheidszorg, en kan afspraken maken met de curatieve zorg over het delen van gegevens die aansluiten bij specifieke doeleinden van Jeugdgezondheidszorg of ouderengezondheidszorg zoals in de wet benoemd. Zoals het op systematische wijze volgen en signaleren van ontwikkelingen in de gezondheidstoestand van jeugdigen en ouderen en van gezondheidsbevorderende en -bedreigende factoren, het ramen van de behoeften aan zorg en de vroegtijdige opsporing en preventie van specifieke stoornissen.

Er is echter geen algemene extra grondslag geregeld voor het delen van tot de persoon herleidbare gegevens tussen de uitvoerders van de zorg en het college of GGD voor die doeleinden. De 'gewone regels' voor uitwisseling van persoonsgegevens (buiten de WPG) zijn derhalve uitgangspunt.

1.6 Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg (Wegiz)

Dit wetsvoorstel ziet op de elektronische uitwisseling van gegevens tussen zorgverleners. Door te verplichten dat gegevens elektronisch uitgewisseld worden (in plaats van niet elek-

tronisch), en eventueel eisen aan taal en techniek te stellen, worden zorgverleners beter in staat gesteld goede zorg verlenen. Het wetsvoorstel is eind april 2021 goedgekeurd in de ministerraad en gaat nu naar de Tweede Kamer.

Met dit wetsvoorstel wordt de verplichting om bij een aangewezen gegevensuitwisseling gegevens elektronisch uit te wisselen, aan de zorgaanbieder opgelegd. Met het aangepaste wetsvoorstel is gekozen om een aanpak per zorgproces. Er is begonnen met vier gegevensuitwisselingen. Bij de Basisgegevensset Zorg gaat het bijvoorbeeld om informatie over allergieën of bloeddruk van de patiënt die ziekenhuizen uitwisselen en bij Beelduitwisseling om MRI- of hartscans.

Ook artsen en apothekers delen onderling medische gegevens. In de gegevensuitwisseling Digitaal Receptenverkeer gaat het erom dat patiënten altijd de juiste medicatie voorschreven krijgen en ontvangen. Tot slot wordt er gewerkt aan Verpleegkundige Overdracht, zodat bijvoorbeeld duidelijk is of iemand bij overplaatsing van een ziekenhuis naar een verpleeghuis nog zelfstandig kan traplopen. Om te zorgen dat al deze medische gegevens verplicht digitaal uitgewisseld kunnen gaan worden, dient er dus eenheid van taal en techniek te komen.

Deze wet regelt ‘enkel’ de verplichting om *digitaal* te gaan uitwisselen en regelt geen grondslagen voor gegevensuitwisseling. Dat wil zeggen dat het in dit onderzoek verder niet relevant is omdat gegevensuitwisselingen altijd op basis van een andere wettelijke regeling zullen plaatshebben. Wel kan het wetsvoorstel en de uitwerking daarvan voor sommige zorgaanbieders duidelijker maken welke gegevensuitwisseling al is aangewezen. Het aangewezen zijn van een gegevensuitwisseling die uit een standaard volgt is op zichzelf ook nog geen grondslag of verplichting tot gegevensuitwisseling. De zorgverlener moet altijd eerst bepalen of er een grondslag voor het verwerken van gegevens is wanneer hij gegevens wil verwerken. En in de gevallen dat de verwerking onder de Wegiz valt moet dat in die gevallen *elektronisch* gebeuren.

1.7 Wkkgz

De Wet kwaliteit, klachten en geschillen zorg regelt de aanpak van klachten, melden van incidenten en kwaliteitsverplichtingen in de zorg. Cliënten hebben een sterkere positie gekregen wanneer er iets mis gaat in de zorgverlening. De cliënt heeft recht op informatie over de kwaliteit van de zorg wanneer hij daarom vraagt. Ook regelt de wet een uitbreiding van de meldplicht van zorgaanbieders betreft geweld in de zorgrelatie en ernstig disfunctioneren. Zorgaanbieders krijgen de ruimte om klachtenregelingen en kwaliteitssystemen te maken die passen binnen hun organisatie. De wet geldt voor alle zorgaanbieders.

Voor dit onderzoek zijn de artikelen 2, 3 en 7 van belang, die gaan over het borgen van goede zorg en aantoonbare kwaliteit van zorg.

Artikel 2

1. De zorgaanbieder biedt goede zorg aan.
2. Onder goede zorg wordt verstaan zorg van goede kwaliteit en van goed niveau:
 - a. die in ieder geval veilig, doeltreffend, doelmatig en cliëntgericht is, tijdig wordt verleend, en is afgestemd op de reële behoefte van de cliënt,

- b. waarbij zorgverleners handelen in overeenstemming met de op hen rustende verantwoordelijkheid, voortvloeiende uit de professionele standaard, waaronder de kwaliteitsstandaard, bedoeld in artikel 1, onderdeel z, van de Zorgverzekeringswet, en
- c. waarbij de rechten van de cliënt zorgvuldig in acht worden genomen en de cliënt ook overigens met respect wordt behandeld.

Artikel 3

De zorgaanbieder organiseert de zorgverlening op zodanige wijze, bedient zich zowel kwalitatief als kwantitatief zodanig van personele en materiële middelen en, voor zover nodig, bouwkundige voorzieningen en, indien hij een instelling is, draagt tevens zorg voor een zodanige toedeling van verantwoordelijkheden, bevoegdheden alsmede afstemmings- en verantwoordingsplichten, dat een en ander redelijkerwijs moet leiden tot het verlenen van goede zorg.

Artikel 7

1. De zorgaanbieder draagt zorg voor systematische bewaking, beheersing en verbetering van de kwaliteit van de zorg.
2. De verplichting van het eerste lid houdt, de aard en omvang van de zorgverlening in aanmerking genomen, in:
 - a. het op systematische wijze verzamelen en registreren van gegevens betreffende de kwaliteit van de zorg op zodanige wijze dat de gegevens voor eenieder vergelijkbaar zijn met gegevens van andere zorgaanbieders van dezelfde categorie;
 - b. het aan de hand van de gegevens, bedoeld in onderdeel a, op systematische wijze toetsen of de wijze van uitvoering van artikel 3 leidt tot goede zorg;
 - c. het op basis van de uitkomst van de toetsing, bedoeld in onderdeel b, zo nodig veranderen van de wijze waarop artikel 3 wordt uitgevoerd.

Artikel 9 Wkkgz gaat over het verwerken van gegevens over incidenten in een register en niet in de eerste plaats over uitwisseling ten behoeve van kwaliteit zoals in dit onderzoek bedoeld.

Op grond van artikel 10 Wkkgz verstrekt de zorgaanbieder aan de cliënt op diens verzoek informatie over de door zorgaanbieder aangeboden zorg, waaronder begrepen de tarieven en de kwaliteit, alsmede over de ervaringen van cliënten met die zorg.

Artikel 7 geeft met name aan hoe de zorgaanbieder zorg draagt voor de naleving van artikel 3 Wkkgz. Het op systematische wijze verzamelen en registreren van gegevens betreffende de kwaliteit van zorg op een manier die vergelijking mogelijk maakt met andere zorgaanbieders is een opdracht tot het verwerken van die gegevens. De wet en het Uitvoeringsbesluit Wkkgz geven geen nieuwe verwerkingsgrondslagen voor het verwerken van persoonsgegevens voor dit doeleinde. Het gaat dus -op basis van deze wet- om gegevens die geanonimiseerd zijn uit het zorgproces.