Gedragscode EGiZ

Elektronische Gegevensuitwisseling in de Zorg

September 2019

Inhoudsopgave

Vooraf

Voor u ligt de Gedragscode Elektronische Gegevensuitwisseling in de Zorg ("Gedragscode EGiZ"), versie 2019.

In deze versie zijn wijzigingen opgenomen in verband met de volgende nieuwe wet- en regelgeving:

- Wet aanvullende bepalingen verwerking van persoonsgegevens in de zorg (Wabvpz, eerder aangeduid als de Wet cliëntenrechten bij elektronische verwerking van gegevens), in werking getreden op 1 juli 2017;
- Besluit elektronische gegevensverwerking door zorgaanbieders (Besluit van 10 november 2017, houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders), in werking getreden op 1 januari 2018;
- Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG, beide van kracht vanaf 25 mei 2018;
- Besluit van de Minister voor Medische Zorg van 27 juni 2019, kenmerk 1529221-190512-WJZ, houdende vaststelling van een bewaartermijn voor logging.

Een eerste conceptversie van deze code is opgesteld door samenwerkende regio-organisaties (EZDA, Rijnmondnet, Zorgring NHN, Sleutelnet, SpitZ Midden-Holland, RSO Haaglanden, IZIT en GERRIT) o.l.v. W. Hodes (directeur GERRIT), met ondersteuning vanuit Nictiz. Vervolgens heeft een werkgroep bestaande uit medewerkers van KNMG, LHV, NHG, VHN , KNMP en Nictiz zich er intensief over gebogen. Juristen van KNMG en Nictiz hebben de voorgestelde aanvullingen en wijzigingen verwerkt in de tekst.

In de versie van november 2014 is de inwerkingtreding van de hoofdstukken 3 en 4 uitgesteld tot 1 januari 2017. In de versie van december 2016 is de inwerkingtreding van de hoofdstukken 3 en 4, met het oog op de invoering van de Wet cliëntenrechten bij elektronische verwerking van gegevens en het Besluit elektronische gegevensverwerking door zorgaanbieders per 1 juli 2017, uitgesteld tot 1 juli 2017. De huidige versie (2019) is aangepast aan de nieuwe wet- en regelgeving die sinds de vorige versie (2016) is ingevoerd.

Deze versie wordt onderschreven door de volgende organisaties:

- De samenwerkende regio-organisaties: SIGRA (voorheen EZDA), Zorgring NHN, Sleutelnet, RSO Haaglanden, Zorgnet Oost (voorheen IZIT), RZCC, REN West-Brabant en GERRIT
- Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst (KNMG), inclusief de federatiepartners:
    - Landelijke Huisartsen Vereniging (LHV)
    - Federatie van Medisch Specialisten (FMS)
    - Specialisten in ouderengeneeskunde (Verenso)
    - Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde (NVAB)
    - Koepel Artsen Maatschappij en Gezondheid (KAMG)
    - Landelijke vereniging van Artsen in Dienstverband (LAD)
    - Nederlandse Vereniging voor Verzekeringsgeneeskunde (NVVG)
    - De Geneeskundestudent
- InEen, vereniging van organisaties voor eerstelijnszorg

- Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie (KNMP)
- Nederlandse Vereniging van Ziekenhuizen (NVZ)

Dit document wordt onderhouden door de KNMG en het Nationaal ICT Instituut in de Zorg (Nictiz). Voor meer informatie kunt u contact opnemen met Sjaak Nouwt (Adviseur gezondheidsrecht KNMG, s.nouwt@fed.knmg.nl).

Tot op heden zijn er de volgende versies van de Gedragscode EGiZ geweest:

- De oorspronkelijke versie (juli 2013);
- De versie van november 2014: hierbij werd de inwerkingtreding van de hoofdstukken 3 en 4 uitgesteld tot 1 januari 2017;
- De versie van december 2016: in deze versie is de inwerkingtreding van de hoofdstukken 3 en 4, met het oog op de invoering van de Wet cliëntenrechten bij elektronische verwerking van gegevens en het Besluit elektronische gegevensverwerking door zorgaanbieders per 1 juli 2017, uitgesteld tot 1 juli 2017.

Inleidende toelichting

Achtergrond

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) dient de zorgaanbieder van elke patiënt een dossier bij te houden. Tegenwoordig gebeurt dat meestal digitaal met behulp van zorginformatiesystemen, zoals huisartsen-informatiesystemen (HIS'en), apotheekinformatie-systemen (AIS'en), ziekenhuis-informatiesystemen (ZIS'en), ketenzorginformatiesystemen (KIS'en), huisartsenpostinformatiesystemen (HAPIS'en), etc.

Veel van de gebruikte systemen hebben een monodisciplinair karakter. Patiënten hebben echter vaak met meerdere zorgaanbieders te maken. De uitwisseling van patiëntgegevens tussen die zorgaanbieders is dan gewenst en vaak zelfs noodzakelijk. In Nederland zijn daarom vele ICT-voorzieningen operationeel, waarmee patiëntgegevens elektronisch kunnen worden uitgewisseld of kunnen worden gedeeld. Het gaat daarbij om regionale, lokale en landelijke voorzieningen die worden beheerd door zorgaanbieders of samenwerkingsverbanden van zorgaanbieders of ook door andere partijen die geen zorgaanbieder zijn.

Bij het uitwisselen van persoonsgegevens moet worden voldaan aan wettelijke voorschriften. Het blijkt daarbij lastig om een goede vertaalslag te maken van wet naar praktijk. Met name het invullen van de patiëntenrechten (o.a. informatieverstrekking en toestemming) blijkt lastig. Oorzaak is de diversiteit aan, vaak door elkaar lopende, voorzieningen, de diversiteit aan behandelrelaties en de schijnbare onmogelijkheid om alle betrokkenen over alle vormen van uitwisseling begrijpelijk te blijven informeren. De Gedragscode EGiZ voorziet in een oplossing daarvoor. Het geeft praktische richtlijnen voor zorgaanbieders en samenwerkingsverbanden om aan geldende regelgeving te kunnen voldoen.

De opstellers van deze Gedragscode zijn zich ervan bewust dat in de praktijk sprake is van een constante zoektocht naar de balans tussen enerzijds het kunnen beschikken over informatie van patiënten teneinde de kwaliteit en patiëntveiligheid te bevorderen en anderzijds de wettelijke verplichtingen tot beveiliging van die informatie en de bescherming van de privacy van patiënten te waarborgen. Die balans bestaat veelal niet uit een vast punt, maar uit een optimaal en dynamisch evenwicht.

Een willekeurig voorbeeld ...

De geschetste problematiek kan worden verduidelijkt aan de hand van de volgende praktijkvoorbeelden:

> *Een huisarts maakt gebruik van een systeem dat is opgenomen in een cluster: zijn systeem werkt met dezelfde database als de systemen van zijn collega's en apotheken in de buurt. De patiëntgegevens (waaronder medicatiegegevens) van een patiënt zijn daardoor voor allen inzichtelijk. Hierover zijn de patiënten nooit geïnformeerd.*
>
> *De huisarts maakt gebruik van het LSP en heeft daarvoor al zijn patiënten aangeschreven, met de vraag of ze toestemming willen geven voor het beschikbaar stellen van hun gegevens via het LSP.*

De huisarts is daarnaast ook aangesloten op een regionaal ketenzorg-systeem. Bij 'doorverwijzing' voor ketenzorg wordt aan bijv. diabetespatiënten gevraagd of zij toestemming geven voor informatiedeling met de medebehandelaren binnen de ketenzorg-organisatie.

Er loopt een project om bovengenoemde ketenzorg-uitwisseling ook via het LSP te laten lopen. De huisarts is huiverig om daarvoor de patiënten opnieuw toestemming te vragen en gaat er eigenlijk vanuit dat e.e.a. binnen de eerder gegeven toestemming kan en mag.

Via zijn Edifact-postbus ontvangt de huisarts al enkele jaren specialistenbrieven, labuitslagen, röntgenonderzoeken en recept-retourberichten, waarover de patiënt eigenlijk nooit is geïnformeerd. Bij twee ziekenhuizen in de buurt kan de huisarts inloggen om rechtstreeks in het ziekenhuissysteem naar informatie over "zijn" patiënten te kijken.

Via een beveiligd portaal worden de labonderzoeken die de huisarts heeft aangevraagd vanuit het laboratorium breder beschikbaar gesteld, bijvoorbeeld aan specialisten die met dezelfde patiënt te maken hebben en aan apotheken.

De huisarts voorziet dat een aantal van zijn patiënten in de nabije toekomst zelf (een deel van) de medische gegevens uit het HIS en uit andere bronnen (ziekenhuisdossiers, zelfmetingen, e.d.) zullen verzamelen, bijhouden en delen in een persoonlijke gezondheidsomgeving (PGO).

Deze praktijkvoorbeelden maken duidelijk dat zorgaanbieders vaak te maken kunnen hebben met vele afzonderlijke uitwisselingssystemen. Ieder systeem kent verschillende deelnemers en verschillende verantwoordelijken. Daarnaast zijn per systeem andere keuzes gemaakt rondom informatie en toestemming. Voor patiënten en zorgaanbieders kan dit tot een onoverzichtelijke en onduidelijke situatie leiden.

Doel en reikwijdte van de Gedragscode

Het doel van de Gedragscode is de formulering van een heldere en toepasbare set (gedrags)regels en bijbehorende normen voor gegevensuitwisseling tussen zorgaanbieders. De wettelijke normen voor gegevensuitwisseling zijn divers en kunnen daardoor onoverzichtelijk en ingewikkeld zijn om toe te passen in de praktijk. Wanneer zorgaanbieders informatie over hun patiënten met andere zorgaanbieders langs elektronische weg delen, kan het soms lastig zijn om in de praktijk een werkbaar evenwicht te vinden tussen privacyregels en goede zorgverlening.

Bij de totstandkoming van de Gedragscode is een aantal uitgangspunten gehanteerd. In de eerste plaats dient de Gedragscode toepasbaar te zijn voor het belangrijkste deel van de bestaande en in de nabije toekomst denkbare oplossingen. In de tweede plaats dienen de normen, mede met het oog op de eventuele indiening hiervan ter goedkeuring bij de Autoriteit Persoonsgegevens (AP) op grond van artikel 40.5 AVG, te voldoen aan de geldende (privacy)regelgeving. Tegelijkertijd moet een balans worden gevonden tussen de handhaving van de rechten van de patiënt en de werkbaarheid in de praktijk.

De Gedragscode is van toepassing op elektronische gegevensuitwisseling. Hieronder valt enerzijds het gebruik van elektronische uitwisselingssystemen voor pull-verkeer. De Gedragscode gebruikt hiervoor – evenals de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (hierna: "Wabvpz") – de term 'Elektronisch Uitwisselingssysteem'. Anderzijds valt ook de verzending van persoonsgegevens via push-verkeer onder de reikwijdte van de Gedragscode.

De Gedragscode is opgesteld om te gelden voor de gehele zorgsector. Daartoe willen de opstellers van de Gedragscode verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, teneinde voldoende representatief te zijn voor de zorgsector. Hieronder verstaan wij het geheel van Zorgaanbieders, Zorginstellingen en Zorgverleners dat zich bezig houdt met de verlening van de eerstelijnszorg, de ziekenhuiszorg, de geestelijke gezondheidszorg, de verpleging, verzorging en thuiszorg, de gehandicaptenzorg en overige zorg (zoals GGD, Arbo, Jeugdzorg, WMO, Ambulancediensten en medische laboratoria).

Informatieverstrekking en toestemming: de hoofdlijnen

In de praktijk roepen met name de regels rondom informatieverstrekking aan de patiënt (de 'Betrokkene') en het verkrijgen van toestemming veel vragen op. De artikelen 5 t/m 8 van de Gedragscode bepalen op welke wijze hiermee moet worden omgegaan. Dit is afhankelijk van de gebruikte methode. Er wordt in dit verband onderscheid gemaakt tussen 'Pull-verkeer' en 'Push-verkeer'.

Pull-verkeer

Van Pull-verkeer is sprake wanneer een Brondossierhouder (zorgaanbieder) gegevens elektronisch beschikbaar stelt voor raadpleging door een of meer andere zorgaanbieders. Het initiatief tot raadpleging ligt dan bij de zorgverlener die de gegevens in het kader van de behandeling nodig heeft en dus een behandelrelatie heeft met de patiënt. Deze zorgverlener wordt in deze Gedragscode aangeduid als de 'Dossierraadpleger'. Voorbeelden van Pull-verkeer zijn inzageportalen en systemen met verwijsindexen (o.a. IHE-XDS en Landelijk Schakelpunt: LSP). Ook inzage door de huisarts van diagnostische gegevens die verzameld zijn in het ziekenhuis is een voorbeeld.

Wanneer sprake is van het beschikbaar stellen van patiëntengegevens die geraadpleegd kunnen worden door andere zorgaanbieders in een samenwerkingsverband of zorggroep, dan valt dat onder de definitie van en bijbehorende regels voor Pull-verkeer. Als een samenwerkingsverband of zorggroep niet alleen voor administratieve ondersteuning van de hulpverleners zorgt, maar bijvoorbeeld ook de waarnemingen regelt en een contract afsluit met de zorgverzekeraar voor de levering van de zorg, dan kan het samenwerkingsverband of die zorggroep mogelijk tevens als een zorgaanbieder worden beschouwd. Als binnen zo'n samenwerkingsverband of zorggroep, die tevens als zorgaanbieder kwalificeert, een elektronisch dossiersysteem wordt gebruikt, dan is dat geen 'elektronisch uitwisselingssysteem' zoals bedoeld in de wet en in deze Gedragscode.

Voor Pull-verkeer geldt dat de Betrokkene voorafgaand Uitdrukkelijke toestemming moet verlenen aan de Brondossierhouder voor het beschikbaar stellen van patiëntgegevens door de Brondossierhouder voor raadpleging door een andere zorgaanbieder. Die toestemming dient gebaseerd te zijn op informatie over deze vorm van gegevensuitwisseling die vooraf aan de Betrokkene moet zijn verstrekt door of onder verantwoordelijkheid van de Brondossierhouder. Die informatie kan op verschillende manieren worden verstrekt, bijvoorbeeld via een (bijlage bij een) toestemmingsformulier of via de webpagina van de zorgaanbieder.

Push-verkeer

Van Push-verkeer is sprake bij verzending van Persoonsgegevens door een Brondossierhouder aan een of meerdere specifieke Zorgaanbieder(s) die een Behandelrelatie heeft/hebben met de Betrokkene, dan wel wanneer een behandelrelatie wordt beoogd. Het initiatief ligt in dit geval bij de

verzender. De ontvangende zorgaanbieder krijgt de gegevens zonder daarvoor het initiatief te hoeven nemen of extra handelingen te hoeven verrichten.

Voorbeelden zijn berichtenverkeer via de Edifact-postbus, ZorgDomein, beveiligde e-mail en verwijs- of overdrachtssystemen. Let wel: het in kopie versturen van berichten aan andere zorgaanbieders die geen behandelrelatie hebben, zoals bijvoorbeeld kan plaatsvinden bij laboratoriumuitslagen, is een uitbreiding van de klassieke informatie-uitwisseling en behoeft toestemming van de patiënt.

Bij Push-verkeer is voorafgaande Uitdrukkelijke toestemming niet vereist. Wel moet de Betrokkene daartegen bezwaar kunnen maken. Daarvoor is het nodig dat de Betrokkene is geïnformeerd over het feit dat er Persoonsgegevens / patiëntengegevens over hem kunnen worden verstrekt aan andere zorgaanbieders. Ook deze informatie kan aan Betrokkenen worden verstrekt via de webpagina van de zorgaanbieder.

De wettelijke verplichting in de Wabvpz om vooraf toestemming te vragen geldt niet voor Push-verkeer. Dit heeft minister Schippers (VWS) in een kamerstuk nader toegelicht:[1]

> *"Er is enige onduidelijkheid ontstaan over de reikwijdte van het wetsvoorstel. Het wetsvoorstel is zowel gericht op push als pull verkeer. Wel kent het wetsvoorstel een aantal bepalingen dat in de uitwerking alleen ziet op pull berichten, namelijk de bepalingen die betrekking hebben op het gebruik van een elektronisch uitwisselingssysteem. Een dergelijk systeem wordt gebruikt voor pull-verkeer. Het betreft de artikelen 15a, 15b, 15e onder a, 15f, 15h. De overige bepalingen, waaronder de logging en beveiligingsmaatregelen gelden zowel voor push als pull berichten."*

Ook op grond van deze Gedragscode EGiZ geldt de eis van uitdrukkelijke toestemming vragen vooraf alleen bij Pull-verkeer en niet bij Push-verkeer. Zie de artikelen 5.5 en 5.6 van deze Gedragscode.

In kamerstuk 33 509, nr. N (pag. 11-12) gaat de minister in op de vraag of gegevens van patiënten geraadpleegd mogen worden als zij weliswaar geen toestemming hebben gegeven daarvoor, maar als er toch een groot gezondheidsbelang is om dat wel te doen. De minister stelt dat in zo'n geval het ontbreken van toestemming moet worden gerespecteerd:

> *"De leden van de CDA-fractie vragen nader in te gaan op de relatie en zo mogelijk de spanning tussen enerzijds de toestemming van de patiënt en anderzijds het vitale belang als bedoeld in artikel 8 van de Wbp (*d.i. artikel 6.1.d AVG*) op grond waarvan een zorgverlener ook zonder toestemming van de patiëntgegevens zou kunnen raadplegen. Kunnen minder zelfredzame mensen er niet de dupe van worden als ze geen toestemming hebben gegeven?*
>
> *Het vitale belang als bedoeld in artikel 8, onderdeel d Wbp (*d.i. artikel 6.1.d AVG*), is geen grondslag om het ontbreken van toestemming in een gewone behandelingsrelatie te "overrulen". Dit vitale belang moet eng worden geïnterpreteerd: het vitale belang (ofwel het leven) van de patiënt of een derde is in het geding en het vragen van uitdrukkelijke toestemming is onmogelijk, bijvoorbeeld vanwege bewusteloosheid. Ook in de WGBO is een dergelijke "nood"-bepaling opgenomen voor het verrichten van medische handelingen zonder toestemming (art. 7:466 BW).*

[1] Kamerstukken I, 2015/16, 33 509, nr. N, pag. 9.

Als cliënten geen toestemming hebben gegeven hun gegevens beschikbaar te stellen via een elektronisch uitwisselingssysteem, zal een (nieuwe) behandelaar van die cliënt geen gegevens over hem kunnen inzien via dat elektronisch uitwisselingssysteem. Op grond van de WGBO kan deze behandelaar wel beschikken over informatie die als push berichten aan hem zijn verstuurd, zoals een verwijzing van de huisarts. Verder heeft de cliënt op grond van art.7:452 BW de verplichting naar beste weten inlichtingen te verstrekken aan de zorgverlener. Voor minder zelfredzame mensen kan dit moeilijk zijn en kan het verlenen van toestemming om via een elektronisch uitwisselingssysteem inzage te geven in zijn gegevens bij andere zorgverleners van grote toegevoegde waarde zijn. Goede voorlichting en eventuele hulp bij het geven van toestemming kan deze mensen helpen om in het belang van hun gezondheid in een betere positie te komen."

De conclusie is dus dat een zorgaanbieder zonder Uitdrukkelijke toestemming geen patiëntendossier of gegevens daaruit via een 'elektronisch uitwisselingssysteem' beschikbaar mag stellen voor elektronische raadpleging door een andere zorgaanbieder, ook niet in spoedgevallen. Artikel 15a Wabvpz prevaleert hier boven de WGBO en de AVG. Dat dit bij zorgaanbieders tot enig zorginhoudelijk ongemak leidt is begrijpelijk, maar dat is een gevolg van de keuze van de wetgever om uitdrukkelijke toestemming te eisen. Voor push-berichten geldt die uitdrukkelijke toestemming overigens niet.

Gedragscode Elektronische Gegevensuitwisseling in de Zorg

Overwegingen

- Zorgaanbieders wisselen in het kader van de zorgverlening via elektronische uitwisselingssystemen persoonsgegevens uit. Zij hechten eraan dat de verwerking van persoonsgegevens in dit kader zorgvuldig en in overeenstemming met de wet geschiedt.

- Op de uitwisseling van persoonsgegevens via elektronische uitwisselingssystemen zijn voorschriften van toepassing uit Boek 7, Titel 7, Afdeling 5 BW (Wet geneeskundige behandelingsovereenkomst (hierna: “WGBO”)), de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (hierna: “Wabvpz”), het Besluit elektronische gegevensverwerking door zorgaanbieders, de Algemene verordening gegevensbescherming (hierna: “AVG”) en de Uitvoeringswet AVG (“UAVG”).

- De WGBO verplicht zorgaanbieders tot het inrichten van een medisch dossier en het geheimhouden daarvan. De AVG beoogt waarborgen te verschaffen ter bescherming van de persoonlijke levenssfeer van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

- Op 1 juli 2017 is de Wet aanvullende bepalingen verwerking van persoonsgegevens in de zorg (Wabvpz) gedeeltelijk in werking getreden. Deze wet vervangt de Wet gebruik burgerservicenummer in de zorg, en bevat de inhoud van het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens (kamerstukken 33509).

- De Wabvpz is aangevuld met het Besluit elektronische gegevensverwerking door zorgaanbieders, dat op 1 januari 2018 in werking is getreden.

- De AVG en de Uitvoeringswet AVG zijn op 25 mei 2018 van kracht geworden.

- Deze gedragscode werkt de hierboven genoemde wettelijke voorschriften uit met het doel om:

    - richtlijnen te geven aan zorgaanbieders en hun samenwerkingsverbanden voor de elektronische uitwisseling van persoonsgegevens;

    - informatie te verschaffen aan personen van wie persoonsgegevens door zorgaanbieders en/of hun samenwerkingsverbanden elektronisch uitgewisseld (zullen) worden.

HOOFDSTUK 1: ALGEMENE BEPALINGEN

Artikel 1 – Begrippen

In deze Gedragscode wordt verstaan onder:

a. AP: de Autoriteit Persoonsgegevens als bedoeld in artikel 6 Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);

b. AVG: Algemene Verordening Gegevensbescherming;

c. Behandelrelatie: de relatie tussen de Betrokkene en de Zorgaanbieder met wie de cliënt een behandelingsovereenkomst als bedoeld in artikel 7:446, eerste lid WGBO heeft, of degene die rechtstreeks betrokken is bij de uitvoering van die behandelingsovereenkomst, of degene die optreedt als vervanger van degene die een behandelingsovereenkomst heeft met de cliënt;

b. Behandelingsovereenkomst: de overeenkomst bedoeld in artikel 7:446 lid 1 WGBO waarbij een natuurlijke persoon of een rechtspersoon, de hulpverlener[2], zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde;

c. Betrokkene: degene op wie een Persoonsgegeven betrekking heeft, in deze Gedragscode de patiënt/cliënt;

d. Brondossier: het dossier als bedoeld in artikel 7:454 lid 1 WGBO dat de Zorgaanbieder laat inrichten en bijhouden of zelf inricht en bijhoudt;

e. Brondossierhouder: de Zorgaanbieder die verantwoordelijk is voor het (laten) onderhouden van het patiëntendossier van een Betrokkene;

f. Derde: ieder, niet zijnde de betrokkene, de Verwerkingsverantwoordelijke, de Verwerker, of enig persoon die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd is om persoonsgegevens te verwerken;

g. Dossierraadpleger: de Zorgverlener die via een Elektronisch Uitwisselingssysteem gegevens van de Betrokkene raadpleegt of onder wiens mandaat gegevens van de Betrokkene worden geraadpleegd ;

h. Elektronische gegevensuitwisseling: pull verkeer via een Elektronisch uitwisselingssystemen, dan wel gegevensuitwisseling via push-verkeer.

i. Elektronisch Uitwisselingssysteem: een systeem waarmee Zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere Zorgaanbieders

[2] Het begrip 'Hulpverlener' in de WGBO komt in grote lijnen overeen met het begrip 'Zorgaanbieder' in de Wkkgz. De Hulpverlener is een natuurlijke persoon of een rechtspersoon, die zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde (artikel 7:446, lid 1 BW). De Zorgaanbieder is een instelling dan wel een solistisch werkende zorgverlener (artikel 1 Wkkgz).

raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een Zorgaanbieder, voor het bijhouden van een elektronisch dossier;

j. Gedragscode: de Gedragscode Elektronische Gegevensuitwisseling in de Zorg (Gedragscode EGiZ);

k. Logging: elektronische vastlegging van acties met betrekking tot het gebruik van een Elektronisch Uitwisselingssysteem en/of een zorginformatiesysteem, met inbegrip van push-verkeer;

l. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;

m. Pull-verkeer: gegevensuitwisseling via een Elektronisch Uitwisselingssysteem waarbij een Brondossierhouder Persoonsgegevens beschikbaar stelt aan een of meer andere Zorgaanbieders voor raadpleging op hun initiatief;

n. Push-verkeer: elektronische verzending van Persoonsgegevens op initiatief van een Brondossierhouder aan een of meerdere specifieke Zorgverlener(s);

o. Samenwerkingsverband: een organisatie, hoofdzakelijk bestaand uit (vertegenwoordigers van) Zorgaanbieders, die gericht is op (ondersteuning van) zorgverlening en die voor dat doel één of meer Elektronische Uitwisselingssystemen in stand houdt;

p. UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming;

q. Uitdrukkelijke toestemming: uiting door de Betrokkene in woord, geschrift of gedrag, waarmee uitdrukking wordt gegeven aan zijn wil toestemming te verlenen voor het verwerken c.q. verstrekken van zijn persoonsgegevens.

r. Verwerkingsverantwoordelijke: de Zorgaanbieder die, de gezamenlijke Zorgaanbieders die, of het Samenwerkingsverband dat, alleen of tezamen met anderen, het doel en de middelen voor de verwerking van Persoonsgegevens ten behoeve van Elektronische gegevensuitwisseling vaststelt;

s. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt;

t. Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

u. Wabvpz: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Dit is de nieuwe naam van de Wet gebruik burgerservicenummer in de zorg, en bevat de inhoud van

het wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens (kamerstukken 33509).

v. WGBO: Wet geneeskundige behandelingsovereenkomst, zoals opgenomen in Boek 7, Titel 7, Afdeling 5 van het Burgerlijk Wetboek;

w. Zorgaanbieder: een instelling dan wel een solistisch werkende zorgverlener, als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz);

x. Zorginstelling: een rechtspersoon die bedrijfsmatig zorg verleent, een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen, als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg;

y. Zorgverlener: een natuurlijke persoon die beroepsmatig zorg verleent, als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg.

Artikel 2 – Toepasselijkheid

De Gedragscode geldt voor de zorgsector en is van toepassing op Elektronische gegevensuitwisseling zoals bedoeld in artikel 1 sub h.

Artikel 3 – Voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens

3.1 Persoonsgegevens worden slechts verwerkt in overeenstemming met het bepaalde in deze Gedragscode en voor zover dat noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene dan wel het beheer van de betreffende instelling of beroepspraktijk.

3.2 De Verwerkingsverantwoordelijke en de Verwerker leggen overeenkomstig artikel 32 AVG, alsmede overeenkomstig het Besluit elektronische gegevensverwerking door zorgaanbieders[3], passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De Verwerkingsverantwoordelijke en de Verwerker leggen aan de personen die zijn belast met het beheer van een Elektronisch Uitwisselingssysteem een geheimhoudingsplicht op.

3.3 De Verwerkingsverantwoordelijke bewaart Persoonsgegevens niet langer dan noodzakelijk voor het doel van de Verwerking van persoonsgegevens. Voor zover Persoonsgegevens deel uitmaken van een patiëntendossier in de zin van de WGBO mogen deze niet langer worden bewaard dan de toepasselijke wettelijke bewaartermijn of zoveel langer als noodzakelijk is voor een goede behandeling van de patiënt.

3.4 Indien twee of meer Zorgaanbieders gezamenlijk de doeleinden en middelen van de verwerking via een Elektronisch Uitwisselingssysteem bepalen, zijn zij gezamenlijke Verwerkingsverantwoordelijken. Zij stellen overeenkomstig art. 26 AVG op transparante wijze

[3] Besluit van 10 november 2017, houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders (Besluit elektronische gegevensverwerking door zorgaanbieders) Stb. 2017, 446.

hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van de AVG vast, met name met betrekking tot de uitoefening van de rechten van de Betrokkene en hun respectieve verplichtingen om de in art. 4.1 bedoelde informatie te verstrekken, door middel van een onderlinge regeling. In de regeling kan een contactpunt voor Betrokkenen worden aangewezen. Uit de bedoelde regeling blijkt duidelijk welke rol de gezamenlijke Verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de Betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de Betrokkene beschikbaar gesteld. Ongeacht de voorwaarden van de bedoelde regeling, kan de Betrokkene zijn rechten uit hoofde van de verordening met betrekking tot en jegens iedere Verwerkingsverantwoordelijke uitoefenen.

3.5 De Verwerkingsverantwoordelijke die te zijnen behoeve Persoonsgegevens laat verwerken door een Verwerker, draagt zorg dat deze overeenkomstig artikel 32 AVG voldoende beveiligingsmaatregelen biedt met betrekking tot de te verrichten verwerkingen. De Verantwoordelijke ziet toe op de naleving van die maatregelen.

3.6 De uitvoering van verwerkingen door een Verwerker wordt geregeld in een schriftelijke overeenkomst tussen de Verwerker en de Verwerkingsverantwoordelijke. Die overeenkomst bevat een nadere omschrijving van het onderwerp en de duur van de verwerking, de aard en de doeleinden van de verwerking, het soort Persoonsgegevens en de categorieën van Betrokkenen, en dient rekening te houden met de specifieke taken en verantwoordelijkheden van de Verwerker in het kader van de te verrichten verwerking en het risico in verband met de rechten en vrijheden van de Betrokkene.

3.7 De Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem benoemt een functionaris voor de gegevensbescherming als bedoeld in artikel 37 AVG. Een instelling als bedoeld in artikel 1, eerste lid, van de Wet kwaliteit, klachten en geschillen zorg, alsmede een Verwerker, die op grote schaal Persoonsgegevens over de gezondheid van Betrokkenen verwerken, benoemen eveneens een functionaris voor de gegevensbescherming als bedoeld in artikel 37 AVG.

Artikel 4 – Rechten van de Betrokkene

4.1 De Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem garandeert de volgende rechten van de Betrokkene:

a. recht op informatie over:

- de werking van het Elektronisch Uitwisselingssysteem en de doeleinden van de Verwerking van Persoonsgegevens die via het Elektronisch Uitwisselingssysteem plaatsvindt;
- de identiteit van de Verwerkingsverantwoordelijke(n) voor het Elektronisch Uitwisselingssysteem;
- indien van toepassing, de contactgegevens van de functionaris voor de gegevensbescherming;
- de rechtsgrond voor de gegevensverwerking;

- de gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of van een derde, indien dat de grondslag is voor de verwerking;
- de periode gedurende welke de persoonsgegevens zullen worden opgeslagen of de criteria ter bepaling van die termijn;
- het recht van de Betrokkene op inzage, verbetering, verwijdering van diens persoonsgegevens, recht op beperking van de verwerking, recht op bezwaar en recht op gegevensoverdraagbaarheid;
- het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit;
- of de verstrekking van persoonsgegevens door de Betrokkene aan de Verwerkingsverantwoordelijke een wettelijke of contractuele verplichting is en wat de mogelijke gevolgen zijn als de Betrokkene de gegevens niet verstrekt;
- de (categorieën van) Persoonsgegevens die door middel van het Elektronisch Uitwisselingssysteem kunnen worden verwerkt;
- de (categorieën van) Zorgaanbieders die via het Elektronisch Uitwisselingssysteem toegang kunnen hebben tot Persoonsgegevens;
- de mogelijkheid om Toestemming voor de Verwerking van Persoonsgegevens te geven, dan wel in te trekken, dan wel om hier bezwaar tegen te maken;
- de aansluiting van nieuwe categorieën Zorgaanbieders of andere substantiële wijzigingen van het Elektronisch Uitwisselingssysteem als bedoeld in artikel 5.3 en de mogelijkheid om de gegeven Toestemming te wijzigen of in te trekken.

b. recht op het geven, het onthouden en het intrekken van toestemming voor de Verwerking van persoonsgegevens of, indien toepasselijk, het maken van bezwaar hiertegen;

c. recht op (elektronische) inzage en kopie, rectificatie en wissing van gegevens alsmede recht op beperking van de verwerking en overdraagbaarheid.

4.2 De in het eerste lid genoemde rechten kunnen worden uitgeoefend door een persoon die bevoegd is om namens de Betrokkene te handelen.

4.3 Is de Betrokkene wilsonbekwaam en twaalf jaar of ouder, dan kan de Betrokkene worden vertegenwoordigd door diens wettelijke vertegenwoordiger (bijvoorbeeld curator of mentor, schriftelijk gemachtigde, echtgenoot, geregistreerde partner of andere levensgezel, tenzij deze persoon dat niet wenst, dan wel een ouder, kind, broer of zus van de Betrokkene, tenzij deze persoon dat niet wenst).

4.4 Is de Betrokkene elf jaar of jonger, dan wordt de Betrokkene vertegenwoordigd door diens wettelijke vertegenwoordiger (bijvoorbeeld curator of mentor, ouders of voogd).

4.5 De Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem kan het recht op informatie en het recht op inzage als bedoeld in artikel 4.1 buiten toepassing laten als dat

noodzakelijk is in het belang van de bescherming van de Betrokkene of van de rechten en vrijheden van anderen.

HOOFDSTUK 2: INFORMATIE EN TOESTEMMING

Artikel 5 – Pull-verkeer

5.1 De Verwerkingsverantwoordelijke verstrekt de in artikel 4.1 sub a genoemde informatie via openbare informatiekanalen, bijvoorbeeld door middel van een online privacyverklaring. De Brondossierhouder maakt deze informatie permanent via elektronische weg toegankelijk en verwijst de Betrokkene naar de vindplaats. De Brondossierhouder verstrekt de in artikel 4.1 sub a genoemde informatie aan de individuele Betrokkene persoonlijk voordat de Brondossierhouder de Betrokkene om uitdrukkelijke toestemming vraagt om diens gegevens beschikbaar te stellen voor raadpleging door andere zorgaanbieders via een elektronisch uitwisselingssysteem.

5.2 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 Betrokkenen, die eerder Uitdrukkelijke toestemming hebben verleend, tenminste vier weken voordat een substantiële wijziging wordt doorgevoerd over deze wijziging alsmede over de mogelijkheid om de gegeven toestemming aan te passen of in te trekken.

5.3 De informatieverstrekking als bedoeld in het eerste en het tweede lid is vormvrij; deze kan mondeling of schriftelijk geschieden.

5.4 De informatieverstrekking aan meerdere Betrokkenen kan ook namens één of meerdere Brondossierhouder(s) gezamenlijk worden uitgevoerd door een Derde.

5.5 De Brondossierhouder stelt gegevens van de cliënt slechts beschikbaar via een Elektronisch Uitwisselingssysteem, voor zover de Brondossierhouder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven.

5.6 Het bepaalde in art. 5.5 geldt niet voor Push-verkeer.

5.7 De Brondossierhouder houdt een registratie bij van de door Betrokkenen verleende toestemming waarbij wordt aangetekend vanaf welk tijdstip de toestemming van kracht is geworden. Een Brondossierhouder kan deze registratie beschikbaar stellen via het Elektronisch Uitwisselingssysteem.

5.8 Raadpleging van gegevens door een Dossierraadpleger vindt slechts plaats nadat de aanwezigheid van een Behandelrelatie tussen de Betrokkene en de Dossierraadpleger is vastgesteld overeenkomstig artikel 8. Indien een Behandelrelatie niet kan worden vastgesteld vindt raadpleging slechts plaats nadat de Dossierraadpleger hiervoor Uitdrukkelijke toestemming heeft verkregen van de Betrokkene.

Artikel 6 – Push-verkeer

6.1 De Verwerkingsverantwoordelijke verstrekt de in artikel 4.1 sub a genoemde informatie via openbare informatiekanalen. De Brondossierhouder maakt deze informatie permanent via elektronische weg toegankelijk en verwijst de Betrokkene naar de vindplaats.

6.2 Push-verkeer kan plaatsvinden zonder Uitdrukkelijke toestemming van de Betrokkene indien Persoonsgegevens uitsluitend worden verzonden aan een of meerdere Zorgaanbieders die een Behandelrelatie hebben met de Betrokkene. Indien niet aan deze voorwaarden is voldaan dient Uitdrukkelijke toestemming van de Betrokkene te worden verkregen. De Brondossierhouder draagt in dat geval zorg voor registratie van de Uitdrukkelijke toestemming en de intrekking hiervan.

6.3 De Betrokkene heeft het recht om bezwaar te maken tegen verzending van hem betreffende Persoonsgegevens via Push-verkeer. De Brondossierhouder registreert en effectueert het door de Betrokkene gemaakte bezwaar.

6.4 Overeenkomstig artikel 66a, eerste lid, Geneesmiddelenwet, mag de apotheker laboratoriumuitslagen die noodzakelijk zijn bij de terhandstelling van een geneesmiddel aan de Betrokkene uitsluitend met de Uitdrukkelijke toestemming van de Betrokkene elektronisch opvragen bij degene die de uitslagen onder zich heeft.

HOOFDSTUK 3: AUTORISATIE

Artikel 7 – Autorisatiebeleid

7.1 De Verwerkingsverantwoordelijke verleent toegang tot Persoonsgegevens via een Elektronisch Uitwisselingssysteem uitsluitend aan:

- de Brondossierhouder(s);
- de Dossierraadpleger, voor zover aan de in deze Gedragscode gestelde toegangsvoorwaarden is voldaan;
- de door de Brondossierhouder of Dossierraadpleger gemandateerde personen;
- de Betrokkene;
- de door de Verantwoordelijke aangewezen functionaris, voor zover noodzakelijk in het kader van het beheer van het Elektronisch Uitwisselingssysteem.

7.2 De Verwerkingsverantwoordelijke stelt een autorisatiebeleid vast voor toegang tot de gegevensverwerking. Dit beleid is er op gericht de Verwerking van persoonsgegevens via een Elektronisch Uitwisselingssysteem te beperken tot hetgeen noodzakelijk is in het kader van de behandeling van de Betrokkene.

7.3 De Verwerkingsverantwoordelijke voorziet in aanvullende waarborgen ten aanzien van de medezeggenschap van patiënten en Zorgaanbieders.

7.4 Het autorisatiebeleid omvat ten minste:

- richtlijnen met betrekking tot het verlenen van toegang tot Persoonsgegevens via het Elektronisch Uitwisselingssysteem, waaronder richtlijnen met betrekking tot mandatering van Zorgverleners met een Behandelrelatie;
- autorisatieprotocollen waarin de reguliere toegang tot Persoonsgegevens via het Elektronisch Uitwisselingssysteem wordt gebonden aan de rol van de Dossierraadpleger.

7.5 Informatie over het autorisatiebeleid wordt permanent via openbare informatiekanalen ter beschikking gesteld.

Artikel 8 – Vastlegging en toetsing Behandelrelatie

8.1 De Verwerkingsverantwoordelijke draagt zorg voor de instandhouding van technische voorzieningen waarmee de Behandelrelatie tussen de Dossierraadpleger en de Betrokkene kan worden vastgesteld. Dit geschiedt door middel van:

a) voorafgaande afleiding van de Behandelrelatie aan de hand van feitelijke omstandigheden; of

b) voorafgaande toetsing aan de hand van een registratie van de Behandelrelatie door de Dossierraadpleger persoonlijk met behulp van een digitale handtekening, of;

c) voorafgaande toetsing aan de hand van een registratie van de Behandelrelatie door de Betrokkene met behulp van een digitale handtekening.

Voorafgaande afleiding van de Behandelrelatie als bedoeld onder sub a) kan plaatsvinden in combinatie met een melding achteraf. Deze melding geschiedt op een (of beide) van de volgende manieren:

- een notificatie aan de Betrokkene, bijvoorbeeld via e-mail of SMS, tenzij Patiënten op andere wijze controle kunnen uitoefenen op onterechte raadplegingen;

- een verslag aan de Brondossierhouder van de raadplegingen die hebben plaatsgevonden, tenzij is afgesproken dat het bestaan van een Behandelrelatie steekproefsgewijs wordt gecontroleerd.

8.2 De registratie of afleiding van een Behandelrelatie als bedoeld in dit artikel is in beginsel geldig voor de duur van één jaar, tenzij anderszins duidelijk is wat de duur van de Behandelrelatie is.

HOOFDSTUK 4: BEVEILIGING

Artikel 9 NEN - normen

9.1 De Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van dat Elektronisch Uitwisselingssysteem.

9.2 Een Zorgaanbieder draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het Elektronisch Uitwisselingssysteem waarop hij is aangesloten.

9.3 De Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem werkt met een zorgserviceprovider die is geautoriseerd op basis van overeenkomstig NEN 7512 vastgestelde criteria.

9.4 Een rechtspersoon, niet zijnde een zorgaanbieder, die een Elektronisch Uitwisselingssysteem beheert en in stand houdt, voldoet aan de volgende voorwaarden:

a. een van de rechtspersoon onafhankelijke organisatie heeft na onderzoek vastgesteld dat de rechtspersoon en het systeem dat hij beheert voldoen aan het bepaalde in NEN 7510 en NEN 7512 en heeft die bevinding opgenomen in een door die organisatie ten behoeve van de rechtspersoon opgesteld audit-rapport;

b. de in onderdeel a bedoelde vaststelling is niet langer dan vijf jaar geleden gedaan.

Artikel 10 - Terminologie

10.1 Bij het vastleggen van beleid, procedures en verantwoordelijkheden als bedoeld in NEN 7510, NEN 7512 of NEN 7513 in documenten, gebruiken de Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem en de Zorgaanbieder de termen en definities als genoemd in NEN 7510, NEN 7512 of NEN 7513.

Artikel 11 - Verantwoording

11.1 De Zorgaanbieder als Verwerkingsverantwoordelijke voor een zorginformatiesysteem en de Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem, vergewissen zich steeds van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens, en verantwoorden zich over de toepassing daarvan bij de inrichting en het gebruik van hun systemen.

Artikel 12 – Identificatie en Authenticatie bij Brondossiers en Elektronische Uitwisselingssystemen

12.1 De Verwerkingsverantwoordelijken voor Brondossiers en voor Elektronische Uitwisselingssystemen zorgen voor technische middelen van voldoende niveau voor het vaststellen en verifiëren van de identiteit van Betrokkenen, Zorgaanbieders en Zorgverleners.

12.2 Voor identificatie en authenticatie van Zorgverleners en medewerkers wordt gebruik gemaakt van passende middelen, zoals de UZI-pas of middelen met een vergelijkbaar beveiligingsniveau.

12.3 Bij het elektronisch uitwisselen tussen Zorgaanbieders van Persoonsgegevens betreffende een Betrokkene wordt gebruik gemaakt van het BSN.

12.4 In verband met de uitoefening van de voorafgaande toetsing van de Behandelrelatie door de Betrokkene, zoals bedoeld in artikel 8.1.c, dient authenticatie van Betrokkenen met tenminste 2-factor authenticatie, zoals DigiD + sms-functie te worden gebruikt, zolang er nog geen algemeen beschikbare 2-factor authenticatie beschikbaar is voor patiënten/cliënten.

Artikel 13 – Logging

13.1 De Zorgaanbieder als Verwerkingsverantwoordelijke voor een zorginformatiesysteem en de Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem dragen er zorg voor dat de Logging van het systeem voldoet aan het bepaalde in NEN 7513.

13.2 De Verwerkingsverantwoordelijke bewaart de gegevens in de Logging gedurende een termijn van tenminste vijf jaar vanaf het moment van het schrijven van de logregel.

13.3 De Verwerkingsverantwoordelijke houdt voorzieningen in stand waarmee de Brondossierhouder of de Betrokkene de Logging kan inzien.

13.4 De Verwerkingsverantwoordelijke stelt een beleid vast met betrekking tot:

- de toegang tot de gegevens in de Logging;
- het uitvoeren van een periodieke controle van de Logging op onbevoegde raadplegingen;
- het uitvoeren van specifieke controles op raadplegingen die hebben plaatsgevonden in noodsituaties, en
- de te volgen procedure bij vermeend of geconstateerd misbruik en/of datalek.

Toelichting per artikel

Artikel 1 – Begrippen

Hieronder wordt een aantal van de in artikel 1 genoemde begrippen nader toegelicht.

Behandelrelatie

Dit begrip wordt voor het eerst omschreven in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). In deze Gedragscode is de definitie uit die wet overgenomen. De Behandelrelatie betreft de relatie in het kader van een geneeskundige behandelingsovereenkomst tussen een Zorgaanbieder (een instelling of een solistisch werkende zorgverlener, zoals bedoeld in de Wet kwaliteit, klachten en geschillen zorg: Wkkgz) en een Betrokkene, patiënt of cliënt.

Van een Behandelrelatie is sprake wanneer er een geneeskundige behandelingsovereenkomst is tussen Betrokkene en een Zorgaanbieder.

Bij een vrijgevestigde Beroepsbeoefenaar kan er gelijktijdig sprake zijn van zowel een Behandelingsovereenkomst (rol Zorgaanbieder) en een behandelrelatie (rol beroepsbeoefenaar).

Van een Behandelrelatie is ook sprake tussen Betrokkene en anderen die kunnen worden aangemerkt als ‘rechtstreeks betrokken bij de uitvoering van de behandelingsovereenkomst’. Dit kunnen personen zijn die werken onder verantwoordelijkheid van een Zorgaanbieder. Zo zullen verpleegkundigen, praktijkondersteuners, doktersassistenten, fysiotherapeuten en artsen die gezamenlijk in een gezondheidscentrum werken hieronder kunnen vallen.

Ook een patholoog, die weefsel moet beoordelen van een patiënt, en een apotheker die voor het zorgvuldig afleveren van een medicijn relevante gegevens nodig heeft van de patiënt, kunnen rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst, evenals de collega vakgenoot aan wie advies gevraagd wordt in het kader van de behandeling. Daarnaast kunnen bijvoorbeeld ook co-assistenten, medisch studenten, biochemici, fysici, paramedici, diëtisten, spelbegeleiders op een kinderafdeling, secretaressen, functionarissen belast met het feitelijk beheer van de patiëntendossiers, functionarissen belast met de financiële afwikkeling, rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst.

Deze personen zullen niet per definitie altijd rechtstreeks betrokken zijn bij de uitvoering van een behandelingsovereenkomst. Dit zal telkens in individuele gevallen moeten worden vastgesteld.

De WGBO kent dit tweeledige criterium: het moet gaan om ‘anderen’ / personen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en de verstrekking (of de toegang) is slechts toegestaan voor zover die verstrekking noodzakelijk is voor de door hen te verrichten werkzaamheden.

Een bekend voorbeeld uit de literatuur is dat het voor een chirurg voor een blindedarmoperatie in de regel niet noodzakelijk is om toegang te hebben tot gegevens over een psychiatrische behandeling.

Door de Registratiekamer, tegenwoordig de Autoriteit Persoonsgegevens (AP) is een aantal criteria geformuleerd op grond waarvan men de kring van rechtstreeks betrokkenen kan bepalen.[4] Deze criteria zijn:

- Is het gebruikelijk in de beroepsgroep om deze andere hulpverlener op deze wijze bij de behandelingsovereenkomst te betrekken?
- Zijn er redelijke alternatieven?
- Heeft de hulpverlener zelf voldoende zeggenschap?
- Zijn privacybeschermende maatregelen getroffen?
- Is deze werkwijze kenbaar bij de patiënt?
- Is deze werkwijze in het belang van de patiënt?
- Is de omvang van de samenwerking voldoende beperkt?

Hieronder worden enkele voorbeelden gegeven van veel voorkomende situaties.

A. Ziekenhuis met daarin vrijgevestigde medisch specialisten, georganiseerd in maatschappen

Betrokkene heeft een geneeskundige behandelingsovereenkomst met het ziekenhuis én gelijktijdig met de afzonderlijke medisch specialisten (rol Zorgaanbieder) die de Betrokkene behandelen. Het personeel in dienst van het ziekenhuis heeft Behandelrelaties met Betrokkene uit hoofde van de Behandelingsovereenkomst met het ziekenhuis én, indien van toepassing, uit hoofde van de Behandelingsovereenkomst tussen Betrokkene en de vrijgevestigde medisch specialist (rol Zorgaanbieder).

B. Ziekenhuis met alle Zorgverleners in dienstverband

De Betrokkene heeft in dit geval één Behandelingsovereenkomst, namelijk met het ziekenhuis. Op basis van deze Behandelingsovereenkomst kunnen er Behandelrelaties bestaan met één of meerdere beroepsbeoefenaren (medisch specialist, arts in opleiding, basisarts, fysiotherapeut, verpleegkundige, etc.) en met het ondersteunend personeel in dienst van het ziekenhuis.

C. Gezondheidscentrum met zorgverleners in dienstverband

De Betrokkene heeft één Behandelingsovereenkomst met het gezondheidscentrum. Uit hoofde hiervan kunnen er Behandelrelaties bestaan met de medewerkers van het Gezondheidscentrum, Zorgverleners en ondersteunend personeel.

D. Groepspraktijk, HOED, Gezondheidscentrum met vrijgevestigde huisartsen

Iedere vrijgevestigde huisarts voor zich heeft de rol van Zorgaanbieder. De Betrokkene heeft een Behandelingsovereenkomst met (in principe) één vrijgevestigd huisarts. Op basis daarvan kunnen er Behandelrelaties bestaan met deze huisarts, met beroepsbeoefenaren in dienst van deze huisarts (HIDHA) en met het ondersteunend personeel in dienst van deze huisarts.

[4] Zie het rapport 'Medicatiebewaking door centrale patiëntenregistraties', d.d. 27 oktober 1998, 95.O.27.

Ook hier is sprake van een complexe situatie, vergelijkbaar met het voorbeeld onder A. Dienstverbanden van medewerkers zijn vaak met een groep van samenwerkende Zorgaanbieders, zoals één of zelfs meer maatschappen.

Behandelingsovereenkomst

Een behandelingsovereenkomst is de overeenkomst tussen een Zorgaanbieder (als juridische entiteit) en een opdrachtgever (meestal de cliënt of patiënt: de Betrokkene). De inhoud van de behandelingsovereenkomst is geregeld in Boek 7, titel 7, afdeling 5 van het Burgerlijk Wetboek (ook wel bekend als de Wet geneeskundige behandelingsovereenkomst: WGBO).

Op grond van de WGBO is de behandelingsovereenkomst – kort gezegd – een overeenkomst, waarbij de hulpverlener (Zorgaanbieder) zich tegenover de opdrachtgever (meestal de patiënt oftewel de Betrokkene) verbindt tot het verrichten van geneeskundige handelingen die rechtstreeks op de patiënt betrekking hebben. Er is dus pas sprake van een geneeskundige behandelingsovereenkomst als het gaat om geneeskundige handelingen gericht op een individu. Door een algemeen, niet op de patiënt gericht advies, bijvoorbeeld op de website van een arts, komt dus geen behandelingsovereenkomst tot stand.

In het algemeen komt een behandelingsovereenkomst tussen de Zorgaanbieder en de patiënt tot stand op het moment dat de patiënt of zijn vertegenwoordiger zich tot de Zorgaanbieder wendt met een concrete hulpvraag gericht op zijn gezondheidssituatie, en de Zorgaanbieder vervolgens op deze vraag ingaat. Daarvan is doorgaans al sprake in de voorfase, als de patiënt in de wachtkamer of wachtruimte op zijn afspraak met de arts, verpleegkundige, assistente wacht. Deze afspraken komen meestal tot stand na telefonisch of ander contact met de assistente of het afsprakenbureau over (de ernst van) de klachten van de patiënt.

Ook als de patiënt op de huisartsenpost, spoedeisende eerste hulp of het spreekuur wacht op zijn beurt voor een consult door de (dienstdoende) arts, is meestal al sprake van de aanvang van een behandelingsovereenkomst. In die gevallen dat daarover twijfel bestaat, bijvoorbeeld als een arts (ongevraagd) noodhulp verleent bij een ongeval op straat, wordt geadviseerd ervan uit te gaan dat een behandelingsovereenkomst tot stand is gekomen. Dat is van belang met het oog op het moeten voldoen aan een aantal patiëntenrechten en plichten die uit de WGBO voortvloeien.

Betrokkene

De Betrokkene is degene op wie een persoonsgegeven betrekking heeft. In de context van de Gedragscode is de Betrokkene vrijwel altijd een patiënt of cliënt aan wie zorg wordt verleend.

In bepaalde situaties kan de Betrokkene zijn rechten niet zelf uitoefenen. Als Betrokkene wordt daarom mede aangemerkt ‘degene die namens de Betrokkene handelt’. Het gaat hier met name om gevallen waarin de Betrokkene wilsonbekwaam is.[5]

[5] In de praktijk komen bij wilsonbekwaamheid vooral vragen naar voren rondom informatie en toestemming. Voor informatie over dit onderwerp wordt verwezen naar de publicatie *Van wet naar praktijk: implementatie van de WGBO Deel 2. Informatie en toestemming.* Hierin wordt specifiek ingegaan op de vertegenwoordiging van minderjarigen en meerderjarige wilsonbekwamen.

Elektronische gegevensuitwisseling

In deze Gedragscode onderscheiden we verschillende vormen van elektronische uitwisseling van patiëntgegevens: enerzijds Pull-verkeer via een Elektronisch Uitwisselingssysteem, en anderzijds gegevensuitwisseling via Push-verkeer. Als (gegevens in) medische dossiers op afstand door een andere zorgaanbieder dan de Brondossierhouder kunnen worden geraadpleegd, is sprake van Pull-verkeer. Als een Brondossierhouder daarentegen het initiatief neemt om patiëntgegevens elektronisch te versturen naar een ander zorgaanbieder, bijvoorbeeld via beveiligde e-mail zoals Zorgmail, dan is sprake van Push-verkeer.

De verschillende vormen van elektronische gegevensuitwisseling zijn in de toelichting vooraf reeds genoemd en worden nog nader uitgewerkt in de toelichting op de artikelen 5 en 6.

Elektronisch Uitwisselingssysteem

Onder een Elektronisch Uitwisselingssysteem wordt in deze Gedragscode, in navolging van artikel 1, sub j, Wabvpz, verstaan: 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.

Voorbeelden hiervan zijn inzageportalen, systemen met verwijsindexen (o.a. LSP, IHE-XDS) en dergelijke. Ook als een huisarts diagnostische gegevens van een patiënt kan raadplegen, welke verzameld en opgeslagen zijn in het ziekenhuis, zal er sprake zijn van een Elektronisch Uitwisselingssysteem.[6]

Een Elektronisch Uitwisselingssysteem kan het mogelijk maken om elektronische toegang tot patiëntendossiers te faciliteren in regio's, maar ook bijvoorbeeld in ketens die niet aan een specifieke regio gebonden zijn, en ook landelijk, zoals door middel van het LSP.

Pull-verkeer

Van Pull-verkeer is sprake indien een Brondossierhouder een dossier, gedeelten van een dossier of Persoonsgegevens uit een dossier, via een Elektronisch Uitwisselingssysteem beschikbaar stelt aan een of meer andere Zorgaanbieders voor raadpleging op hun initiatief.

Om als Brondossierhouder dossiers of onderdelen daaruit beschikbaar te stellen via systemen die Pull-verkeer mogelijk maken is Uitdrukkelijke toestemming van de patiënt vereist. Een andere Zorgaanbieder mag alleen dossiers of gegevens daaruit raadplegen als die zelf een Behandelrelatie met de patiënt heeft en voor zover raadpleging voor die Behandelrelatie noodzakelijk is. Dat moet ook voor de patiënt verifieerbaar zijn.

Systemen die Pull-verkeer mogelijk maken kunnen nader worden onderverdeeld in:

- systemen die gebruik maken van een verwijsindex;

- systemen die rechtstreeks toegang verlenen tot een bronsysteem;

[6] Bron: Juridische Factsheet Wet cliëntenrechten bij elektronische uitwisseling van gegevens (VWS).

- combinaties van bovengenoemde systemen.

Ad 1: systemen die gebruik maken van een verwijsindex;

Voorbeelden van systemen met een verwijsindex zijn:

- het Landelijk Schakelpunt (LSP), d.i. de infrastructuur voor gegevensuitwisseling van de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ);

- een regionaal portaal met een centrale patiëntindex, waarin verwijzingen naar verschillende te raadplegen dossiers zijn opgenomen;

- beeldenuitwisseling tussen ziekenhuizen op basis van de IHE-XDSi-standaard

Ad 2: systemen die rechtstreeks toegang verlenen tot een bronsysteem

Voorbeelden van systemen die rechtstreekse toegang mogelijk maken zijn:

- een portaaloplossing vanuit het ziekenhuis, waarbij huisartsen in een elektronisch patiëntendossier kunnen kijken;

- een portaal van een diagnostisch centrum, waarbij Zorgaanbieders rechtstreeks in bijvoorbeeld labgegevens kunnen kijken.

Ad 3: combinaties van bovengenoemde systemen

Combinaties zijn bijvoorbeeld te zien bij ketenzorginformatiesystemen (KIS), waarbij sprake kan zijn van zowel een index functie als ook opslag van (deels gedupliceerde) gegevens.

Push-verkeer

Van Push-verkeer is sprake bij verzending van Persoonsgegevens door een Brondossierhouder aan een of meer specifieke Zorgaanbieder(s) die een (beoogde) Behandelrelatie heeft/hebben met de Betrokkene.

Voorbeelden van systemen waarmee Push-verkeer wordt mogelijk gemaakt zijn:

- elektronisch berichtenverkeer, bijvoorbeeld op basis van de Edifact-standaard, dat bedoeld is als vervanging van reeds lang bestaande papieren correspondentie (bijv. een labuitslag of specialistenbrief aan de huisarts);

- elektronisch berichtenverkeer via (beveiligde) e-mail, zoals ZorgMail, SecureMail, E-zorg, Voltage, Zivver;

- systemen voor verwijzing en overdracht zoals ZorgDomein, Point, etc.

Samenwerkingsverband

Een Samenwerkingsverband wordt in deze Gedragscode gedefinieerd als ‘een organisatie, hoofdzakelijk bestaande uit (vertegenwoordigers van) Zorgaanbieders die gericht is op (ondersteuning van) zorgverlening en die voor dat doel één of meer Elektronische Uitwisselingssystemen in stand houdt’.

Met ‘een organisatie, hoofdzakelijk bestaande uit (vertegenwoordigers van) Zorgaanbieders’ wordt bedoeld dat het verband is opgericht door Zorgaanbieders en dat de aangesloten partijen ook (hoofdzakelijk) Zorgaanbieders zijn. De organisatie zelf hoeft niet uit (louter) Zorgaanbieders te bestaan. De aard en omvang van Samenwerkingsverbanden kan zeer uiteenlopend zijn.

Het is van belang dat een Samenwerkingsverband naar buiten toe makkelijk identificeerbaar en aanspreekbaar is voor alle betrokkenen. Een Samenwerkingsverband is daarom bij voorkeur een rechtspersoon zoals een vereniging, een stichting of een besloten vennootschap (B.V.). Hoewel de maatschap en de vennootschap onder firma (VOF) formeel geen rechtspersoonlijkheid bezitten, zijn ook dit geschikte rechtsvormen. Wanneer sprake is van een gegevensverwerking waarbij meer dan enkele tientallen Zorgaanbieders betrokken zijn, is rechtspersoonlijkheid zonder meer gewenst.

Voorbeelden van Samenwerkingsverbanden zijn:

- de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ);
- regionale samenwerkingsverbanden op het gebied van zorg-ICT, zoals Rijnmondnet, EZDA, IZIT, Stichting GERRIT, Zorgring Noord-Holland Noord, Sleutelnet, RSO Haaglanden;
- huisartsenposten met hun deelnemende huisartsen;
- ketenzorggroepen: samenwerkende instellingen/Zorgaanbieders, gericht op het leveren van ketenzorg en meer inmiddels: ouderenzorg, GGZ;
- stichtingen van samenwerkende Zorgaanbieders die een Regionaal Schakelpunt beheren of daarvoor als opdrachtgever optreden.

Verwerkingsverantwoordelijke

De Gedragscode verstaat onder de Verwerkingsverantwoordelijke ‘de Zorgaanbieder die, de gezamenlijke Zorgaanbieders die, of het Samenwerkingsverband dat, alleen of tezamen met anderen, het doel en de middelen voor de verwerking van Persoonsgegevens ten behoeve van Elektronische Gegevensuitwisseling vaststelt’. Zodoende wordt aangesloten bij het begrip Verwerkingsverantwoordelijke in de Algemene verordening gegevensbescherming (AVG). Het gaat hier met nadruk om de partij die doel en middelen van de Elektronische Gegevensuitwisseling vaststelt. Daarnaast is iedere Zorgaanbieder die een dossier bijhoudt ten aanzien van dit dossier aan te merken als een Verwerkingsverantwoordelijke in de zin van de AVG.

Als Verwerkingsverantwoordelijke kunnen, afhankelijk van de situatie, zowel de individuele Zorgaanbieder, de Zorgaanbieders gezamenlijk, de Zorginstelling, als het Samenwerkingsverband worden aangemerkt.

Verwerker

Overeenkomstig artikel 4, sub 8, AVG is een Verwerker "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt". De Verwerker verwerkt Persoonsgegevens uitsluitend in opdracht van de Verwerkingsverantwoordelijke.[7] De Verwerker handelt overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. De verwerking door een Verwerker moet worden geregeld in een overeenkomst of andere rechtshandeling die de Verwerker aan de Verwerkingsverantwoordelijke bindt. De BOZ-partijen en de Landelijke Huisartsen Vereniging hebben model verwerkersovereenkomsten gepubliceerd die hiervoor gebruikt kunnen worden.[8]

Bij Elektronische Gegevensuitwisseling in de zorg komt gegevensverwerking door Verwerkers vaak voor. Voorbeelden van partijen die veelvuldig optreden als Verwerker zijn netwerkdienstverleners en leveranciers van informatiesystemen.

Wanneer gebruik wordt gemaakt van een Verwerker die zich bevindt buiten de Europese Unie dienen de regels met betrekking tot doorgifte van persoonsgegevens aan derde landen in acht te worden genomen.

Zorgaanbieder

De Gedragscode spreekt in een groot aantal gevallen van de 'Zorgaanbieder'. Dit is de solistisch werkende Zorgverlener of de Zorginstelling waarmee een patiënt een Behandelingsovereenkomst heeft. Het gaat altijd om een Zorginstelling of een solistisch werkende Zorgverlener in de zin van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz).

Wanneer een Zorgverlener in loondienst is bij een Zorginstelling komt de Behandelingsovereenkomst tot stand met de Zorginstelling. De Zorginstelling is in dat geval dus de Zorgaanbieder in de zin van deze Gedragscode.

Zorginstelling

Een Zorginstelling is een rechtspersoon die bedrijfsmatig zorg verleent, een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen, als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg. Bij een Zorginstelling is sprake van een organisatorisch verband waarin de zorg wordt verleend. Dat verband wordt in stand gehouden door de Zorgaanbieder, die de zorg in dat verband zelf verleent of doet verlenen. In een Zorginstelling wordt de zorg verleend door meer dan één persoon. Voorbeelden zijn:[9]

[7] Artikel 29 AVG.
[8] Brancheorganisaties Zorg, 'Modelverwerkersovereenkomst voor de zorgsector'. Nieuwsbericht BOZ, 13 december 2017. Op internet: https://www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/ (laatst geraadpleegd op 14 maart 2018). Landelijke Huisartsen Vereniging (LHV), 'Voorbeeld verwerkersovereenkomst'. Op internet: https://www.lhv.nl/service/verwerkersovereenkomst-beslisschema-checklist-en-voorbeeldovereenkomst (alleen voor leden; laatst geraadpleegd op 14 maart 2018).
[9] Bron: Memorie van toelichting Wkkgz, Kamerstukken II, 2009/10, 32 402, nr. 3, p. 90.

- de apotheker die de cliënten laat bedienen door een of meer apothekersassistenten die bij hem in dienst zijn;

- de ondernemer die een kliniek exploiteert en het werk laat doen door meerdere specialisten die als zelfstandige voor hem de zorg verlenen met eventueel een specialistenmaatschap die voor hem de zorg verleent;

- het samenwerkingsverband van enkele als zelfstandige werkende fysiotherapeuten;

- de maatschap van een aantal specialisten die gezamenlijk een kliniek exploiteren;

- de stichting die een kliniek exploiteert en het werk laat doen door meerdere specialisten en een specialisten-BV;

- een huisartsenpost;

- een zorggroep;

- een zorgverzekeraar die ervoor heeft gekozen (een deel van) de verzekerde zorg te doen verlenen door eigen medewerkers.

Zorgverlener

Veel van de bepalingen in de Gedragscode richten zich niet tot een organisatie of instelling maar tot een individuele persoon (in juridische zin: de 'natuurlijke' persoon). Deze wordt in de Gedragscode consequent aangeduid als de 'Zorgverlener'. Zodoende wordt aangesloten bij de definitie van het begrip 'Zorgverlener' in de Wkkgz en in het spraakgebruik in de gezondheidszorg. In de Gedragscode EGiZ is de Zorgverlener gedefinieerd als de natuurlijke persoon die beroepsmatig zorg verleent. Het gaat altijd om natuurlijke personen, d.w.z. mensen van vlees en bloed. Een huisartsenpraktijk waarbinnen een assistente lichte vormen van zorg verleent, zoals oren uitspuiten, is bijvoorbeeld aan te merken als een zorginstelling omdat in dat geval sprake is van 'een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen'.[10]

In de praktijk wordt ook vaak het begrip 'hulpverlener' gebruikt. Deze term wordt ook toegepast in de Wet geneeskundige behandelingsovereenkomst (WGBO), maar heeft daar een hele specifieke betekenis. De hulpverlener in de zin van de WGBO is de natuurlijke persoon of de rechtspersoon met wie de opdrachtgever een behandelingsovereenkomst heeft (zie art. 446 lid 1 WGBO). Dit komt overeen met het later bij wetgeving ingevoerde begrip Zorgaanbieder.

Artikel 2 – Toepasselijkheid

Deze Gedragscode is van toepassing op alle vormen van Elektronische gegevensuitwisseling zoals bedoeld in artikel 1 sub h. De Gedragscode geldt zodoende voor een grote verscheidenheid van praktijksituaties en informatiesystemen. In de Inleidende Toelichting is reeds een hoofdindeling gegeven (zie p. 6-7).

[10] Kamerstukken II, 2009/10, 32 402, nr. 3, p. 91. Zie ook de definitie van 'zorginstelling' in artikel 1, sub x.

De reikwijdte van de Gedragscode is dus in principe zeer ruim. Alle vormen van Elektronische gegevensuitwisseling in de zorg vallen hier onder. De koepels hebben met elkaar afgesproken om de code in elk geval bindend te hanteren voor de Elektronische gegevensuitwisseling *tussen* Zorginstellingen en tussen Zorginstellingen en andere Zorgaanbieders, zoals solistisch werkende Zorgverleners.

Artikel 3 – Voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens

Het betreft hier een aantal algemene bepalingen die grotendeels overeenkomen met de verplichtingen van de Verwerkingsverantwoordelijke voortvloeiend uit de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), de Wet geneeskundige behandelingsovereenkomst (WGBO) en het Besluit elektronische gegevensverwerking door zorgaanbieders.[11] Voor de volledigheid zijn deze bepalingen in de Gedragscode overgenomen.

Beveiligingsplicht (art. 3.2)

Alle maatregelen in organisatie, mensen en techniek die nodig zijn voor het waarborgen van de vertrouwelijkheid zijn opgenomen in de NEN 7510 (deel 1 en 2) en de ISO27001 en ISO27002.

Verwerkingsverantwoordelijken en Verwerkers zijn op grond van artikel 32 AVG verplicht ‘passende technische en organisatorische maatregelen’ te treffen ‘om een op het risico afgestemd beveiligingsniveau te waarborgen’. Een nadere uitwerking van deze beveiligingsplicht uit artikel 32 AVG is te vinden in de AP ‘Richtsnoeren beveiliging van persoonsgegevens’ (februari 2013) en in de normen NEN7 510 (deel 1 en 2: Informatiebeveiliging in de zorg), NEN 7512 (Vertrouwensbasis voor gegevensuitwisseling) en NEN 7513 (Vastleggen van acties op elektronische patiëntendossiers). De Inspectie Gezondheidszorg en Jeugd verplicht een groot aantal organisaties de NEN 7510 na te leven.

Voor alle personen die het operationeel beheer van de verschillende elementen van de gegevensuitwisseling uitvoeren en uit dien hoofde toegang hebben tot de data in de gegevensuitwisseling dient voorzien te zijn in een geheimhoudingsplicht. Beveiliging dient ‘state of the art’ te zijn en dus regelmatig te worden ge-update. Dit betekent dat moet worden aangesloten bij de NEN 7510 en dat risicoanalyses moeten worden gedaan.

Het Besluit elektronische gegevensverwerking door zorgaanbieders schrijft voor dat Zorgaanbieders moeten zorgen voor een veilig en zorgvuldig gebruik van hun zorginformatiesysteem en voor een veilig en zorgvuldig gebruik van het Elektronisch Uitwisselingssysteem waarop zij zijn aangesloten. Daartoe moeten zij handelen overeenkomstig het bepaalde in de NEN-normen 7510 en 7512 (artikel 3, tweede lid).

[11] Besluit van 10 november 2017, houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders (Besluit elektronische gegevensverwerking door zorgaanbieders) Stb. 2017, 446.

Artikel 4 – Rechten van de Betrokkene

De in artikel 4 genoemde rechten komen grotendeels overeen met de bepalingen hierover in de Algemene verordening gegevensbescherming (AVG) en de Wet geneeskundige behandelingsovereenkomst (WGBO).

Artikel 4.1 sub a: recht op informatie

Het recht van de Betrokkene om informatie te krijgen over de gegevensverwerking correspondeert met de verplichting tot informatieverstrekking van de Verwerkingsverantwoordelijke op grond van artikel 13 en 14 AVG en artikel 15c, lid 1, Wabvpz. In de Algemene toelichting op hoofdstuk 2 is dit nader toegelicht. De in artikel 4.1 sub a genoemde elementen vormen een nadere uitwerking van deze verplichting die specifiek is toegespitst op gegevensuitwisseling in de zorg.

Hoewel er waarschijnlijk nooit sprake zal zijn van een wettelijke of contractuele verplichting voor Betrokkenen om gegevens te verstrekken aan een Verwerkingsverantwoordelijke, kan men Betrokkenen in dit verband ook informeren over argumenten waarom patiënten beter wel toestemming zouden geven om hun gegevens elektronisch beschikbaar te stellen via een Elektronisch Uitwisselingssysteem.

Artikel 4.1 sub b: toestemming en bezwaar

Het uitgangspunt dat de Betrokkene in staat moet worden gesteld zijn toestemming te verlenen is hieronder toegelicht in de Algemene toelichting op hoofdstuk 2. De Uitdrukkelijke Toestemming van de Betrokkene is vereist voordat een Brondossierhouder de patiëntgegevens van die Betrokkene beschikbaar mag stellen via een Elektronisch Uitwisselingssysteem (voor pull-verkeer; zie art. 5.5 van deze Gedragscode). De Verwerkingsverantwoordelijke moet die verleende toestemming kunnen aantonen (art. 7 lid 1 AVG). De Betrokkene heeft het recht om zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming dient even eenvoudig te zijn als het geven ervan (art. 7 lid 3 AVG).

De mogelijkheid om bezwaar te maken geldt wanneer gegevensuitwisseling plaatsvindt op basis van veronderstelde toestemming, zoals het geval is bij Push-verkeer (zie ook de toelichting bij artikel 7).

Deze bezwaarmogelijkheid moet worden onderscheiden van het recht op bezwaar van artikel 21 AVG, dat alleen van toepassing is als de verwerking plaats vindt op grond van artikel 6.1.e (taak van algemeen belang op openbaar gezag) of 6.1.f (gerechtvaardigd belang) AVG. In het kader van een geneeskundige behandelingsovereenkomst zal de grondslag echter veelal een andere zijn, te weten: art. 6.1.b (uitvoering van een overeenkomst) of 6.1.c (uitvoering wettelijke verplichting).

Artikel 4.1 sub c: inzage, (elektronische kopie) rectificatie, wissing, beperking verwerking en overdraagbaarheid

Het recht op inzage in en afschrift van de gegevens in het dossier volgt uit artikel 15 AVG en, meer specifiek, uit artikel 7:456 van de Wet geneeskundige behandelingsovereenkomst (WGBO). Na de wijzigingen vanwege de Aanpassingswet AVG (kst. 34 939) en de wijziging van de WGBO (kst. 34 994) luidt de laatstgenoemde bepaling als volgt:

'De hulpverlener verstrekt aan de patiënt desgevraagd inzage in en afschrift van de gegevens uit het dossier, bedoeld in artikel 454. De verstrekking blijft achterwege voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander.'

De zin 'De hulpverlener mag voor de verstrekking van het afschrift een redelijke vergoeding in rekening brengen' is door de Aanpassingswet AVG geschrapt uit art. 7:456, waardoor het verstrekken van inzage en afschrift kosteloos moet worden verleend.

Wanneer de Betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt (art. 15 lid 3 AVG). Ook heeft de Betrokkene, onder bepaalde voorwaarden, een recht op overdraagbaarheid (dataportabiliteit) van persoonsgegevens (artikel 20 AVG).

Daarnaast voorziet art. 15d Wabvpz in een recht op kosteloze elektronische inzage in en afschrift van gegevens uit een patiëntendossier. Deze bepaling zou niet eerder dan op 1 juli 2020 in werking treden, maar op grond van art. 15 lid 3 AVG geldt het recht op kosteloze elektronische inzage en afschrift dus al vanaf 25 mei 2018.

Dit recht op inzage en afschrift omvat ook het recht op inzage en afschrift van persoonsgegevens in een verwijsindex en in een logbestand. In de Gedragscode is als uitgangspunt genomen dat het inzagerecht, genoemd in artikel 4.1 sub c, ook geldt ten aanzien van de gegevens in de Logging. Dit recht op inzage in logbestanden volgt uit artikel 456 WGBO en artikel 15.1.c AVG ("recht op informatie over de ontvangers aan wie de persoonsgegevens zijn verstrekt").

Het correctierecht volgt uit artikel 16 AVG. De Betrokkene heeft het recht om van de Verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Ook kan hij onvolledige persoonsgegevens aanvullen door middel van een aan de Verwerkingsverantwoordelijke gerichte verklaring. Een dergelijk recht op aanvulling van het dossier bestaat op grond van art. 7:454, lid 2 ook jegens de Brondossierhouder.

De Brondossierhouder is op grond van art. 19 AVG in beginsel verplicht om iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis te stellen van elke rectificatie of wissing van persoonsgegevens of beperking van de verwerking overeenkomstig art. 16, art. 17 lid 1 en art. 18 AVG, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

Het recht op wissing van persoonsgegevens (artikel 17: 'recht om vergeten te worden') geldt in beginsel niet voor patiëntendossiers. Dit volgt onder meer uit artikel 17, lid 3 AVG:

'De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:

(…)

c. om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9 lid 2, punten h) en i) en artikel 9, lid 3.'

Niettemin volgt het recht op vernietiging van (gegevens uit) patiëntendossiers uit artikel 455 WGBO. De tekst van deze bepaling luidt in zijn volledigheid (na wijziging via de Aanpassingswet AVG en het wetsvoorstel tot wijziging van de WGBO): [12]

> *'1. De hulpverlener vernietigt de gegevens uit het dossier na een daartoe strekkend schriftelijk of elektronisch verzoek van de patiënt.*
>
> *2. Lid 1 geldt niet voor zover het verzoek gegevens betreft waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de patiënt, alsmede voor zover het bepaalde bij of krachtens de wet zich tegen vernietiging verzet.'*

Het hier bedoelde recht op vernietiging heeft betrekking op de gegevens in het patiëntendossier in de zin van artikel 454 WGBO. De gegevens in de Logging zijn niet aan te merken als onderdeel van het patiëntendossier aangezien zij geen betrekking hebben op de behandeling. Voor deze gegevens geldt het vernietigingsrecht uit de WGBO dus niet.

Vooralsnog gaat de Gedragscode EGiZ er van uit dat de gegevens in de Logging ook niet onder het recht op wissing vallen, aangezien deze gegevens als 'noodzakelijk met het oog op het beheer van de betreffende instelling of beroepspraktijk' kunnen worden beschouwd (artikel 30 UAVG, onder verwijzing naar artikel 9 lid 2 onderdeel h AVG).

Algemene toelichting op Hoofdstuk 2: Informatie en toestemming

De wettelijke regels rondom het verstrekken van informatie aan de patiënt over de gegevensverwerking en het verkrijgen van toestemming roepen in de praktijk veel vragen op bij zorgaanbieders en andere betrokken partijen. Hieronder wordt hierop nader ingegaan.

Informatieverstrekking

Voordat persoonsgegevens via een uitwisselingssysteem mogen worden verwerkt, door deze beschikbaar te stellen voor elektronische raadpleging door een andere zorgaanbieder, (dus anders dan door de Brondossierhouder in zijn eigen brondossier) dient de Verwerkingsverantwoordelijke hiervoor toestemming van de Betrokkene te verkrijgen. Daarvoor is het eerst nodig de Betrokkene informatie te verstrekken over zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd. Dit volgt uit de artikelen 13 en 14 Algemene Verordening Gegevensbescherming (AVG). Daarnaast dient de Verwerkingsverantwoordelijke nadere informatie te verstrekken voor zover dat, gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de Betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen (art. 13 lid 2 en art. 14 lid 2 AVG).

De AVG maakt onderscheid tussen de verzameling van gegevens bij de Betrokkene zelf (art. 13 AVG) en verkrijging op een andere wijze (art. 14 AVG). In het laatste geval is de verplichting tot informatieverstrekking niet van toepassing voor zover dit onmogelijk blijkt of een onevenredige inspanning zou vergen (art. 14 lid 5 sub b AVG) of indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven (art. 14 lid 5 sub c AVG). Aangezien deze situaties zich slechts in

[12] Via de Aanpassingswet AVG is de reactietermijn van drie maanden geschrapt en dient voortaan 'onverwijld' te worden gereageerd op een verzoek tot vernietiging van de gegevens.

uitzonderlijke gevallen voor zullen doen, zijn deze bepalingen niet overgenomen in de Gedragscode EGiZ.

Praktische problemen
Informatieverstrekking conform de AVG stuit in de praktijk vaak op verschillende praktische bezwaren. In de eerste plaats is, mede gezien de vele vormen van gegevensuitwisseling, vaak onduidelijk op wie de verplichting tot informatieverstrekking rust. Bovendien bestaan bij Zorgaanbieders en Zorgverleners vaak onduidelijkheden en interpretatieverschillen over de wijze waarop de informatieverstrekking moet plaatsvinden.

In de tweede plaats leidt het herhaaldelijk en afzonderlijk verstrekken van informatie over verschillende bestaande toepassingen in sommige gevallen tot een voor de Betrokkene (en de Zorgverlener) onbegrijpelijke situatie. Te veel informatie of informatie van te veel verschillende bronnen kan tot onbegrip en weerstand leiden. Is de Betrokkene opgenomen in meerdere systemen, dan is het onderscheid hiertussen vaak ook moeilijk te begrijpen.

In de derde plaats sluit informatieverstrekking door de Verwerkingsverantwoordelijke niet altijd goed aan bij de belevingswereld van de Betrokkene. De Verwerkingsverantwoordelijke kan voor de Betrokkene een onbekende derde zijn waarmee hij geen relatie heeft.

Ten slotte brengt de verplichting tot informatieverstrekking voor de Verwerkingsverantwoordelijke vaak een aanzienlijke inspanning met zich mee, terwijl hieraan eveneens hoge kosten zijn verbonden.

De Gedragscode wil op een aantal punten duidelijkheid scheppen. Allereerst wordt de verplichting tot informatieverstrekking gelegd bij de Brondossierhouder, zijnde de Zorgaanbieder die verantwoordelijk is voor het dossier. Dit is voor de patiënt het meest logisch en begrijpelijk. De Brondossierhouder is immers de Zorgaanbieder aan wie de patiënt zijn gegevens toevertrouwt en die wettelijk verplicht is een patiëntendossier bij te houden als hulpverlener in de zin van de WGBO.

Consequentie van dit uitgangspunt is, dat een patiënt die met meerdere Zorgaanbieders te maken heeft, in principe ook door al die Zorgaanbieders zal moeten worden geïnformeerd. Indien gewenst kunnen de Brondossierhouders de informatie dan gezamenlijk (laten) verstrekken, mits maar duidelijk is namens welke Zorgaanbieders de informatieverstrekking plaatsvindt. Dit is in artikel 5.4 verwoord. Voorbeelden zijn:

- De apotheker en huisartsen in een bepaald gebied spreken met elkaar af dat zij gaan aansluiten op het LSP. De apotheker stuurt hierover iedereen een brief, namens hemzelf en de medewerkende huisartsen;

- Samenwerkende zorgverleners binnen een diabetes-ketenzorggroep besluiten specifieke gegevens met elkaar te delen in het kader van de behandeling van diabetespatiënten. Besloten wordt dat de huisarts de patiënten hierover informeert, namens hemzelf en de aangesloten zorgverleners.

Een uitzondering geldt voor Push-verkeer (zie de toelichting bij artikel 6).

De Gedragscode regelt voor verschillende typen systemen hoe de informatieverstrekking in zijn werk gaat. Dit wordt hieronder bij de artikelen 5 en 6 nader toegelicht.

Samenhang met zeggenschap van de Betrokkene
De verplichting tot informatieverstrekking hangt nauw samen met de voorschriften rondom de zeggenschap van de Betrokkene (d.w.z. het geven dan wel onthouden van toestemming). In de eerste plaats dient duidelijk te zijn waarop de toestemming betrekking heeft: het moet dus gaan om een welbepaalde gegevensverwerking of beperkte categorie van gegevensverwerkingen. Anders gezegd kan de Betrokkene de vereiste toestemming alleen geven indien hij op de juiste wijze geïnformeerd is over de betekenis en de reikwijdte hiervan. Hetzelfde geldt voor de situatie waarin wordt uitgegaan van 'veronderstelde toestemming '. Ook daar heeft de Betrokkene informatie nodig om te bepalen of hij al dan niet bezwaar wil maken.

Het toestemmingvereiste
Zorgaanbieders zijn op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) verplicht om van elke patiënt een dossier bij te houden (de WGBO spreekt in dit verband overigens van de 'hulpverlener', maar in deze Gedragscode hanteren wij in de meeste gevallen het ook in andere wetgeving gebruikte begrip 'zorgaanbieder').

Zodra een voorziening wordt gecreëerd om elektronische uitwisseling tussen Zorgverleners mogelijk te maken en waarvoor Persoonsgegevens worden vastgelegd, bijvoorbeeld in een verwijsindex, is sprake van een nieuwe, zelfstandige registratie of beschikbaarstelling van Persoonsgegevens. Hiervoor is in beginsel toestemming van de patiënt nodig.

De verplichting om toestemming te verkrijgen vloeit voort uit de Algemene Verordening Gegevensbescherming (AVG). De medische gegevens die in de gezondheidszorg via elektronische weg worden uitgewisseld zijn vrijwel altijd aan te merken als 'persoonsgegevens' en vallen daarmee binnen de werkingssfeer van de AVG. De AVG verstaat onder Persoonsgegevens 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene") […]' (art. 4 onderdeel 1) AVG). (zie ook de gelijkluidende definitie in artikel 1 sub l van de Gedragscode).

De verwerking van persoonsgegevens is op grond van de AVG slechts toegestaan indien hiervoor een zogenaamde 'verwerkingsgrond' aanwezig is (art. 6 AVG). Voor de verwerking van persoonsgegevens in een Elektronisch Uitwisselingssysteem is de uitdrukkelijke toestemming van de Betrokkene doorgaans de meest voor de hand liggende verwerkingsgrond (zie art. 6 lid 1 sub a AVG en art. 9 lid 2 sub a) AVG).

De Verwerkingsverantwoordelijke moet de verleende toestemming kunnen aantonen (art. 7 lid 1 AVG). De wetgever heeft deze verplichting destijds in de Memorie van Toelichting bij de Wet bescherming persoonsgegevens als volgt toegelicht:

> *De verantwoordelijke heeft rekening te houden met een dubbele bewijslast. In de eerste plaats moet bij twijfel bewezen kunnen worden, dat een bepaalde toestemming is verleend en waarvoor. Daarnaast zal zo nodig bewezen moeten kunnen worden, dat de toestemming aan de gestelde eisen voldoet. Daarbij zal de verantwoordelijke ook moeten kunnen aantonen, dat hij bijvoorbeeld op het punt van informatieverstrekking aan de betrokkene, alles heeft gedaan wat redelijkerwijs van hem mocht worden verwacht.*

Als de toestemming niet aan bovenstaande vereisten voldoet is zij nietig. […][13]

De Autoriteit Persoonsgegevens (AP) heeft in 2014 een onderzoek gedaan naar de toestemming voor de uitwisseling van medische persoonsgegevens via het Landelijk Schakelpunt (LSP). Het rapport dat de AP hierover publiceerde bevat de volgende passage over het aantonen van toestemming:

Ter controle van (a) de documenten betreffende de toestemming en (b) het informatiemateriaal dat door de zorgverlener is verstrekt, heeft het CBP het volgende beoordelingskader gehanteerd:

Ad a. Aantonen toestemming

Het CBP acht de toestemming voldoende aangetoond wanneer door VZVZ per getrokken BSN uit de verwijsindex één of meer van de volgende documenten is overgelegd:

- *een door de patiënt ondertekend toestemmingsformulier voor het elektronisch uitwisselen van medische gegevens via het LSP;*
- *een schermprint van het informatiesysteem van de zorgverlener waaruit is af te leiden dat de patiënt akkoord is met elektronisch uitwisselen van medische gegevens via het LSP;*
- *een aantekening in het dossier van de patiënt dat toestemming is verkregen voor het elektronisch uitwisselen van medische gegevens via het LSP. In dat geval is een handtekening of paraaf van de zorgverlener vereist.*

Daarnaast dient het document, waaruit de toestemming blijkt, in alle gevallen te zijn gedateerd.[14]

De AP stelde in dit onderzoek uiteindelijk vast dat de VZVZ voldoende technische en organisatorische waarborgen had getroffen om te bewerkstelligen dat alleen persoonsgegevens worden verwerkt van patiënten die daarvoor toestemming hadden verleend. Daarbij woog de AP mee dat de VZVZ de volgende waarborgen had getroffen:

- *in de technische eisen van de infrastructuur was vastgelegd dat alleen gegevens van patiënten wier toestemming is geregistreerd worden uitgewisseld;*
- *de VZVZ had aan aangesloten zorgverleners instructies gegeven over het verkrijgen van toestemming en was met hen contractueel overeengekomen dat de VZVZ controle uitoefent op naleving van afspraken hierover in de gebruiksovereenkomst. VZVZ verklaarde daarnaast controles te (laten) uitvoeren die ook zien op de toestemmingsprocedures. Ten slotte moeten alle verkregen toestemming in het XIS worden vastgelegd conform contractuele eisen en GBZ-eisen.[15]*

Artikel 5 – Pull-verkeer

Artikel 5.1 bepaalt dat een Brondossierhouder, voordat hij patiëntgegevens beschikbaar stelt voor elektronische raadpleging door een andere zorgaanbieder, de Betrokkene persoonlijk dient te

[13] Kamerstukken II, 1997-1998, 25 892, nr. 3, p. 67 (Memorie van Toelichting Wet bescherming persoonsgegevens).
[14] Rapport College bescherming persoonsgegevens d.d. 1 september 2014, *Onderzoek naar de toestemming voor de uitwisseling van medische persoonsgegevens via het Landelijk Schakelpunt* (z2012-779).
[15] Idem, p. 7.

informeren. Dit volgt onder meer uit beslissingen van de Autoriteit Persoonsgegevens (AP).[16] De eis dat de Betrokkene persoonlijk dient te worden geïnformeerd houdt in dat hij individueel benaderd moet worden. De informatieverstrekking kan mondeling of schriftelijk geschieden.

De Verwerkingsverantwoordelijke voor een Elektronisch Uitwisselingssysteem mag de in art. 4.1 sub a genoemde informatie via openbare informatiekanalen verstrekken, bijvoorbeeld in een online privacyverklaring. De Brondossierhouder dient vervolgens Betrokkenen te verwijzen naar die informatie.

Omdat ervoor gekozen is de informatieverstrekking omtrent het Elektronisch Uitwisselingssysteem te laten plaatsvinden door de Brondossierhouder, is het logisch om ook de verkrijging van toestemming via de Brondossierhouder te regelen. Uitgangspunt is nu dat de patiënt toestemming geeft aan de Brondossierhouder om via een Elektronisch Uitwisselingssysteem Persoonsgegevens beschikbaar te stellen. Hiermee verkrijgt de Verwerkingsverantwoordelijke tegelijkertijd toestemming om via het Elektronisch Uitwisselingssysteem Persoonsgegevens te verwerken. Voorwaarde hiervoor is uiteraard dat de informatieverstrekking conform artikel 5 adequaat is verlopen en dat ook aan de overige bepalingen van de Gedragscode wordt voldaan.

Wijze van informeren bij uitbreiding van de omvang van de verwerking
Zorginformatiesystemen zijn sterk in ontwikkeling. Het komt dan ook regelmatig voor dat de omvang van de Verwerking wordt uitgebreid. Zo kan de dataset die via het Elektronisch Uitwisselingssysteem beschikbaar wordt gemaakt worden uitgebreid. Ook is het mogelijk dat een nieuwe categorie van Zorgaanbieders toegang krijgt tot het systeem, of dat er een koppeling plaatsvindt met een andere voorziening.

In artikel 5.2 is bepaald dat de Zorgaanbieder informatie verstrekt aan de Betrokkene die eerder Uitdrukkelijke toestemming hebben verleend, over de betreffende uitbreiding, alsmede over de mogelijkheid om de gegeven toestemming, bedoeld in artikel 5.6 aan te passen of in te trekken. Dit is in overeenstemming met artikel 15c, lid 1, Wabvpz. Het is uiteraard niet verboden om ook Betrokkenen te informeren die nog geen toestemming hebben verleend.

Uitdrukkelijke toestemming
Artikel 5.5 van deze Gedragscode bevat de hoofdregel dat bij het delen van elektronische medische dossiers of gegevens daaruit, de patiënt vooraf Uitdrukkelijke toestemming dient te geven. Deze hoofdregel komt overeen met artikel 15a lid 1 Wabvpz. Deze toestemmingseis geldt voor het delen van die gegevens via Pull-verkeer, dus niet als gegevens via Push-verkeer worden gestuurd naar een andere Zorgaanbieder.

De toestemming zoals bedoeld in art. 15a lid 1 Wabvpz moet een ‘vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting’ zijn, waarmee de patiënt door middel van een verklaring of een ondubbelzinnige actieve handeling aanvaardt dat er persoonsgegevens over hem worden verwerkt

[16] Dit betreft in het bijzonder de onderzoeken die de AP heeft uitgevoerd bij de Centrale Huisartsen Post te Gorinchem (CHP) en bij de Stichting Schakelpunt Informatie Transmurale Zorg Midden-Holland (SPITZ-MH). Zie ‘CBP: Twee regionale elektronische patiëntendossiers in strijd met de wet. Patiënten niet geïnformeerd over opname van hun gegevens.’ Persbericht Autoriteit Persoonsgegevens, 27 mei 2009.

(art. 4 sub 11 AVG). Op grond van art. 4 sub 11 AVG geldt sinds 25 mei 2018 dat die toestemming 'specifiek' moet zijn. Niet te verwarren met de eis van 'gespecificeerde toestemming', welke op 1 juli 2020 in werking zou treden, maar waarvan de inwerkingtreding tot nader order is uitgesteld.[17] Onder 'specifieke' toestemming kan in verband met de elektronische gegevensuitwisseling worden verstaan dat de Brondossierhouder de Patiënt voorafgaand aan het verlenen van toestemming in elk geval informeert over de (soorten) Persoonsgegevens die elektronisch beschikbaar zullen worden gesteld aan welke (categorieën van) Dossierraadplegers.

De Verwerkingsverantwoordelijke moet voorts kunnen aantonen dat de Patiënt Uitdrukkelijke Toestemming heeft gegeven. Het verzoek om toestemming moet in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke een eenvoudige taal worden gepresenteerd. De Betrokkene moet de Uitdrukkelijke Toestemming te allen tijde kunnen intrekken op een even eenvoudige wijze als waarop de toestemming is gegeven (art. 7 AVG).

Praktische adviezen voor het opstellen van een folders en brieven
Huisartsen kunnen bij het opstellen van een informatiefolder gebruik maken van hulpmiddel 3 (Informatiefolder voor patiënten) uit de KNMG Leidraad gegevensbeheer Huisartsen Dienstenstructuren. Apothekers kunnen gebruik maken van de patiëntenfolder "Persoonsgegevens, medicijnen en uw privacy" van de KNMP.

De VZVZ, NVZ en het Elkerliek Ziekenhuis hebben samen een standaardfoldertekst voor ziekenhuizen opgesteld waardoor met één folder en formulier toestemming kan worden gevraagd voor de gegevensuitwisseling via verschillende uitwisselingssystemen.[18]

Artikel 6 – Push-verkeer

Van Push-verkeer is sprake bij verzending van Persoonsgegevens door een Brondossierhouder aan een of meerdere specifieke Zorgaanbieder(s) die een (beoogde) Behandelrelatie heeft/hebben met de Betrokkene. Indien sprake is van een Behandelrelatie kan op grond van artikel 457 lid 2 Wet geneeskundige behandelingsovereenkomst (WGBO) worden uitgegaan van veronderstelde toestemming. Hiermee wordt een uitzondering gemaakt op het algemene uitgangspunt dat Uitdrukkelijke toestemming van de Betrokkene dient te worden verkregen.

De genoemde uitzondering geldt onder andere voor recept- en afleverberichten en voor de terugkoppeling van behandelresultaten. Wanneer gegevens in kopie worden gezonden aan partijen die geen Behandelrelatie hebben, dient daarvoor wel Uitdrukkelijke toestemming te worden verkregen. Hiervan kan bijvoorbeeld sprake zijn bij het versturen van kopieën van labuitslagen aan anderen dan de aanvrager.

[17] Zie ook de VWS-Brochure Elektronische gegevensuitwisseling in de zorg. Op internet: https://www.rijksoverheid.nl/onderwerpen/rechten-van-patient-en-privacy/veranderingen-zorgververleners-verwerking-medische-gegevens en de kamerbrief van minister Bruins van 4 oktober 2019 met bijlagen. Op internet: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z18953&did=2019D39458.
[18] Bron: https://www.vzvz.nl/ziekenhuizen/toestemming-vragen-voor-andere-zorgverleners/toestemming-vragen-voor-verschillende

De uitzondering van artikel 6.2 geldt ook voor situaties waarin gegevens worden verstrekt aan een maatschap of een huisartsengroep terwijl nog niet bekend is welke specialist of huisarts de patiënt zal behandelen.

Artikel 7 – Autorisatie

Binnen een Elektronisch Uitwisselingssysteem worden aan Zorgaanbieders bevoegdheden toegekend met betrekking tot – onder meer - het aanmelden en opvragen van patiëntgegevens. Om te verzekeren dat deze bevoegdheden niet verder reiken dan voor de behandeling van de Betrokkene noodzakelijk is, dienen de Zorgaanbieders gezamenlijk een autorisatiebeleid te formuleren. Dit autorisatiebeleid koppelt bevoegdheden van Zorgaanbieders aan hun zorginhoudelijke rol. Hiervoor kan in het bijzonder aansluiting worden gezocht bij hoofdstuk 9 van NEN norm 7510:2017-2 over toegangsbeveiliging.

In 2013 publiceerde de Autoriteit Persoonsgegevens een onderzoeksrapport over de toegang tot EPD's.[19] Op 15 december 2016 bood minister Schippers (VWS) een rapport van PBLQ over beveiliging van patiëntgegevens aan de Tweede Kamer aan.[20] Naar aanleiding van dit laatste rapport hebben NVZ, NFU, ZKN en GGZ Nederland een 'Actieplan Informatiebeveiliging in de medisch-specialistische zorg en geestelijke gezondheidszorg' opgesteld.[21] In eerste instantie richt dit plan zich op ziekenhuizen, GGZ instellingen en zelfstandige klinieken. In dit plan worden concrete activiteiten benoemd waarmee koepelorganisaties en/of zorgaanbieders medio 2017 aan de slag zijn of gaan. GGZ Nederland kent sinds maart 2014 een Handreiking Autorisatie tot het Elektronisch Patiëntendossier.[22] In deze handreiking zijn de eisen opgenomen waaraan de autorisaties voor het EPD moet voldoen.

Voor de eerstelijns zorgaanbieders hebben de LHV, het NHG, InEen, de KNMP en expertisecentrum Nictiz onder de noemer 'Beveiliging eerstelijns informatiesystemen' samengewerkt aan het opstellen van een handreiking bestaande uit 2 delen met heldere en implementeerbare eisen ten aanzien van authenticatie en autorisatie (deel 1) en Logging (deel 2).[23]

Indien landelijke autorisatieprotocollen beschikbaar zijn voor een bepaalde toepassing, dient hierbij te worden aangesloten. Betrokkenen moeten altijd worden geïnformeerd over het vigerende autorisatiebeleid en de systemen moeten zodanig worden ingericht, dat het beleid ook wordt nageleefd.

Artikel 8 – Vastlegging en toetsing Behandelrelatie

De Verwerkingsverantwoordelijke dient er voor zorg te dragen dat maatregelen worden getroffen om raadpleging van Persoonsgegevens door anderen dan Zorgaanbieders met een Behandelrelatie tegen te gaan. De meest betrouwbare toetsing van de Behandelrelatie kan worden bereikt door de

[19] College bescherming persoonsgegevens, Toegang tot digitale patiëntendossiers binnen zorginstellingen. Den Haag: juni 2013.
[20] PBLQ, Onderzoek naar de beveiliging van patiëntgegevens. Den Haag: 1 december 2016.
[21] NVZ, NFU, ZKN, GGZ Nederland, Actieplan Informatiebeveiliging in de medisch-specialistische zorg en geestelijke gezondheidszorg (14 juni 2017).
[22] Vindplaats: http://www.ggz-connect.nl/bericht/4935/handreiking-autorisaties-epd (laatst geraadpleegd op 27 juli 2017).
[23] Nictiz, NHG, LHV, InEen, KNMP, Handreiking Informatiebeveiliging voor eerstelijnsinformatiesystemen. DEEL 1 AUTHENTICATIE EN AUTORISATIE en DEEL 2 TOEGANGSLOG (1 januari 2017). Op internet: https://www.lhv.nl/actueel/nieuws/voorwaarden-waaraan-de-beveiliging-van-uw-his-moet-voldoen (laatst geraadpleegd op 27 juli 2017).

Betrokkene hierin zelf een rol te geven. Artikel 8 lid 1 sub c noemt daarom de mogelijkheid om de Betrokkene de Behandelrelatie zelf te laten vastleggen met behulp van een digitale handtekening. Hiermee wordt vooruitgelopen op de praktijk. Deze gang van zaken verdient de voorkeur maar komt, voor zover bekend, nog nauwelijks voor.

Het Burgerlijk Wetboek (BW) stelt een aantal eisen aan de digitale handtekening (daar 'elektronische handtekening' genoemd) wil deze dezelfde rechtskracht hebben als een handgeschreven handtekening (zie art. 3:15a BW). De gebruikte authenticatiemethode moet voldoende betrouwbaar zijn, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval. Specifieke eisen zijn benoemd in artikel 3:15a lid 2 BW.

Alternatief voor de bovengenoemde mogelijkheid zijn toetsing aan een vastlegging door de Dossierraadpleger zelf of een afleiding op basis van feitelijke omstandigheden. Als gebruik gemaakt wordt van de mogelijkheid van toetsing aan een vastlegging door de Dossierraadpleger, dan moet de Verwerkingsverantwoordelijke voldoende waarborgen hebben. Die waarborgen kunnen bestaan uit het contractueel vastleggen en technisch effectueren van bijvoorbeeld een Single-Sign-On koppeling vanuit het systeem waarin de Behandelrelatie is vastgelegd, of een expliciete bevestiging van deze toetsing van de behandelrelatie door de Dossierraadpleger, die in het uitwisselingssysteem gelogd wordt en zo controleerbaar is voor de Verwerkingsverantwoordelijke Brondossierhouder.

Een voorbeeld van een feitelijke omstandigheid is een bestaande afspraak die een patiënt heeft met een zorgverlener. Als de Behandelrelatie wordt afgeleid op basis van feitelijke omstandigheden, dan dient, als aanvullende waarborg, een melding achteraf plaats te vinden teneinde de afgeleide Behandelrelatie achteraf te kunnen controleren. In plaats van notificatie van de Betrokkene, is het ook toegestaan om via een patiëntenportaal inzage in de logging voor de Patiënt aan te bieden waardoor de Patiënt controle kan uitoefenen op onterechte raadplegingen. In plaats van het sturen van een verslag aan de Brondossierhouder kan ook worden afgesproken om een periodieke controle van de logging te houden waarbij steekproefsgewijs het bestaan van de behandelrelatie wordt gecontroleerd. In de praktijk wordt op deze wijze reeds de toestemmingsregistratie getoetst.

Het tweede lid van artikel 8 bepaalt dat de registratie of afleiding van een Behandelrelatie in beginsel slechts geldig is voor de duur van één jaar, tenzij anderszins duidelijk is wat de duur van de Behandelrelatie is. Met de laatste bijzin wordt onder andere gedoeld op huisartsen en apothekers. Zij hebben doorgaans immers een doorlopende Behandelrelatie met de Betrokkene, bijvoorbeeld via een inschrijving op naam.

Artikel 9 – NEN normen

Een Elektronisch Uitwisselingssysteem moet voldoen aan de NEN normen voor informatiebeveiliging in de zorg: NEN 7510:2017 en NEN 7512:2015. Deze NEN normen zijn door NHG, LHV, InEen en KNMP geoperationaliseerd via de BEIS-normen (Beveiligingseisen voor eerstelijns informatiesystemen) die voor de eerste lijn als veldnorm geldt.

Een Zorgaanbieder kan Verwerkingsverantwoordelijke zijn voor een Elektronisch Uitwisselingssysteem. Bij een rechtspersoon die een Elektronisch Uitwisselingssysteem beheert of in stand houdt, kan het ook gaan om een dienstverlener of leverancier van een zorginformatiesysteem.

Artikel 12 – Identificatie en authenticatie bij Brondossiers en Elektronische Uitwisselingssystemen

Het identificeren van een persoon ('zeggen wie je bent') vindt plaats aan de hand van een uniek kenmerk, zoals een uniek nummer. Bij het authentiseren van een persoon ('bewijzen wie je bent') wordt gecontroleerd of de gebruiker daadwerkelijk de persoon of entiteit is die deze beweert te zijn. Voor het vaststellen van de identiteit van Zorgverleners, medewerkers en Betrokkenen dient gebruik te worden gemaakt van zogenaamde 'zware authenticatie' of een 'hoog zekerheidsniveau', bestaande uit 2 van de drie volgende onderdelen: weten, hebben en zijn.

- iets wat men weet: gebruikersnaam, wachtwoord, PIN, TAN;
- iets wat men heeft: token, smartcard, SIM/telefoon;
- iets wat men 'is' vingerafdruk, iris, gezichtsgeometrie, handpalmdoorbloeding.

In Nederland is zware authenticatie bijvoorbeeld ingevuld door gebruik van de UZI-pas (zorgverleners) en DigiD + sms (burgers). Deze methode is vrij beschikbaar gesteld door de overheid. Voor de voorafgaande toetsing van de Behandelrelatie door de Betrokkene, zoals bedoeld in artikel 8.1.c, wordt ter authenticatie van Betrokkenen bij voorkeur gebruik gemaakt van een twee-factor authenticatie waarbij de sleutel face-to-face wordt uitgegeven. Zolang er nog geen algemeen beschikbare 2-factor authenticatie beschikbaar is voor patiënten/cliënten mag DigiD + sms worden gebruikt.[24]

Artikel 13 – Logging

De gegevens in een patiëntendossier zijn van belang voor de gezondheid van patiënten en tegelijkertijd privacygevoelig van aard. Het is daarom belangrijk om te allen tijde te kunnen achterhalen wie er toegang heeft gehad tot een patiëntendossier en volgens welke regels die toegang is verkregen.[25] Voor dit doel dient een gebruiksregistratie te worden bijgehouden, ook wel aangeduid als 'Logging'.

De plicht om te loggen vloeit voort uit op de Verwerkingsverantwoordelijke en de Verwerker rustende de algemene wettelijke verplichting om een op het risico afgestemd beveiligingsniveau te waarborgen (art. 32 AVG).

Het Nederlands Normalisatie Instituut heeft een norm vastgesteld met betrekking tot Logging (NEN 7513 'Logging – Vastleggen van acties op elektronische patiëntendossiers'). Deze norm is van toepassing op verschillende informatiedomeinen in de gezondheidszorg: regionaal informatienetwerk, patiëntdossier in een apotheek of huisartsenpraktijk, persoonlijk zorgdossier, e.d.

Verwerkingsverantwoordelijken voor een Elektronisch Uitwisselingssysteem, maar ook Verwerkingsverantwoordelijken voor een zorginformatiesysteem, zoals een systeem voor het bijhouden van medische dossiers, zijn op grond van artikel 5, lid 1 van het Besluit elektronische

[24] Zie ook: Nictiz, NHG, LHV, InEen, KNMP, Handreiking Informatiebeveiliging voor eerstelijnsinformatiesystemen. DEEL 1 AUTHENTICATIE EN AUTORISATIE (1 januari 2017), pag. 10. Op internet: https://www.lhv.nl/actueel/nieuws/voorwaarden-waaraan-de-beveiliging-van-uw-his-moet-voldoen (laatst geraadpleegd op 27 juli 2017).
[25] Zie ook ABRvS 30 november 2011, LJN: BU6383. In deze uitspraak is het recht op inzage in de logging door de rechter erkend.

gegevensverwerking door zorgaanbieders verplicht om ervoor te zorgen dat hun systeem voldoet aan de voorwaarden van NEN-norm 7513:2010.

In artikel 13.2 wordt een algemene minimum bewaartermijn voor logbestanden vermeld van vijf jaar, vanaf het moment dat de logregel wordt geschreven. Deze minimum termijn volgt uit het Besluit bewaartermijn voor logging.[26]

De Gedragscode stelt als eis, dat er een adequate Logging moet zijn, waarop controleprocedures van toepassing zijn en waarbij in elk geval de Brondossierhouder kan zien wie gegevens uit 'zijn' dossiers heeft geraadpleegd. De Verwerkingsverantwoordelijke moet hiervoor zorg dragen.

Aandachtspunt bij controleprocedures vormt de opvolging van mogelijk misbruik. Hierbij is te denken aan het volgende:

- bij vermeend misbruik: contact met de Zorgaanbieder voor hoor en wederhoor;
- bij geconstateerd misbruik: melding aan Dossierraadpleger, Brondossierhouder, de Betrokkene en de leidinggevende of organisatie waar de Dossierraadpleger deel van uitmaakt of aan verbonden is;
- in geval van een datalek ('inbreuk in verband met persoonsgegevens'): volg interne procedure bij een vermoeden van een datalek, met mogelijk melding aan de Autoriteit Persoonsgegevens en aan Betrokkenen (zie art. 1 onderdeel 12 en art. 33 en 34 AVG) .

[26] Besluit van de Minister voor Medische Zorg van 27 juni 2019, kenmerk 1529221-190512-WJZ, houdende vaststelling van een bewaartermijn voor logging. *Staatscourant* 10 juli 2019, nr. 38007.