Privacy in de zorg

Privacy in de zorg

Een praktische gids voor zorgverleners,
managers en juristen

Sophie Hendriks | Ivette Janssen | Barbara Krol
Jurriaan Dane | Martin Hemmer | René Huigen | Ruben Tienhooven

Privacy in de zorg. Een praktische gids voor zorgverleners, managers en juristen
Sophie Hendriks, Ivette Janssen, Barbara Krol, Jurriaan Dane, Martin Hemmer, René Huigen, Ruben Tienhooven

ISBN: 9789492952622
NUR: 860
www.berghauserpont.nl

Voorwoord

Privacy compliance kan tot complexe vraagstukken leiden. Dit geldt bij uitstek in de zorg. Allereerst worden in de zorg onvermijdelijk grote hoeveelheden gevoelige (persoons)gegevens verwerkt waarvoor een zwaarder beschermingsregime geldt. Ten tweede is naast de Algemene verordening gegevensbescherming (AVG) specifieke nationale wet- en regelgeving van toepassing die invloed heeft op de rechtmatige verwerking van (persoons)gegevens in de zorg.

Met dit boek wordt beoogd een overzicht te geven van de belangrijkste privacyvraagstukken die in de (somatische) gezondheidszorg spelen. Het boek is bedoeld voor mensen met een professionele interesse voor privacy in de zorg. Getracht is om het boek niet alleen een nuttig naslagwerk te laten zijn voor juristen of functionarissen voor gegevensbescherming (FG's) in de zorg, maar ook om zorgverleners en managers in de zorg zonder juridische achtergrond een goed overzicht te bieden van privacyrechtelijke kwesties waar iedere zorginstelling mee te maken krijgt.

De auteurs houden zich vanuit verschillende perspectieven in hun dagelijkse werk bezig met privacyrecht: als juristen in een ziekenhuis, als privacy- en IT-consultants en als advocaten IT- en privacyrecht. Gepoogd is om de ervaring van de auteurs onderdeel te maken van het boek door middel van praktijkvoorbeelden en tevens middels een casus die als rode draad door de hoofdstukken loopt.

De totstandkoming van het boek is een intensief traject geweest. De relatief snelle ontwikkeling van wet- en regelgeving en in de jurisprudentie noopten regelmatig tot updates van reeds gerealiseerde onderdelen. De inhoud van het boek is eind april 2022 gefinaliseerd, ontwikkelingen na die tijd zijn dus niet meegenomen.

Er is gezocht naar een gulden middenweg tussen diepgang en toegankelijkheid. Sommige behandelde vraagstukken zijn complex en kennen geen eenduidig antwoord. De auteurs hopen dat aangedragen oplossingen en suggesties een positieve bijdrage zullen leveren aan de ontwikkeling van het privacyrecht in de zorg.

Inhoud

1 Inleiding

1.1 Aanleiding voor dit boek

De bescherming van de privacy is een vanzelfsprekend uitgangspunt in de geneeskunde sinds de Eed van Hippocrates die rond 400 voor Christus werd opgesteld. Die eed bevat het volgende onderdeel:

Al hetgeen mij ter kennis komt in de uitoefening van mijn beroep of in het dagelijks verkeer met mensen en dat niet behoort te worden rondverteld, zal ik geheim houden en niemand openbaren.

De internationale Declaration of Geneva van de World Medical Association voegt daar expliciet aan toe dat de geheimhouding ook geldt na het overlijden van de patiënt.[1] De meest recente artseneed die wordt gebruikt op Nederlandse geneeskundefaculteiten stelt ten aanzien van privacy kortweg: "Ik zal geheim houden wat mij is toevertrouwd".[2] Het afleggen van de eed is geen wettelijke verplichting of voorwaarde voor het verkrijgen van een BIG-registratie en ook zonder het afleggen van de artseneed zijn artsen – en andere zorgverleners – aan geheimhouding gebonden; de geheimhoudingsplicht is namelijk op verschillende plekken in de wet verankerd.[3]

Het recht op privacy, ook wel het recht op eerbiediging van de persoonlijke levenssfeer, is veel ruimer dan de geheimhoudingsplicht in de zorg. Het is een universeel mensenrecht dat zowel in internationale verdragen als in de Grondwet is vastgelegd.[4] Het 'klassieke' privacybegrip was gericht op bescherming van de persoonlijke levenssfeer tegen inmenging, vooral door de overheid. Tegenwoordig omvat het recht op privacy ook de positieve verplichting om de privacy van de burger actief te beschermen.

Het begrip privacy omvat zowel informationele privacy (het (medisch) beroepsgeheim en gegevensbeschermingsrecht) als fysieke privacy (het recht op onaantastbaarheid van het lichaam), ruimtelijke privacy (huisrecht), privacy m.b.t. communicatie (briefgeheim) en relationele privacy (recht op familie- en gezinsleven).

In de gezondheidszorg speelt het recht op privacy op verschillende manieren een belangrijke rol. Zo impliceert lichamelijk onderzoek van de cliënt een inbreuk op diens recht op lichamelijke integriteit, kan bij institutioneel verblijf in een verpleeghuis of psychiatrisch ziekenhuis de ruimtelijke privacy in het geding komen en kan het verwerken van gezondheidsgegevens leiden tot een schending van de informationele privacy. Daarom is de bescherming van deze aspecten van privacy ook verankerd in nationale gezondheidswetgeving.

1 https://www.wma.net/wp-content/uploads/2018/07/Decl-of-Geneva-v2006-1.pdf.

2 KNMG, *De Nederlandse Artseneed,* mei 2019, p. 7.

3 Art. 88 Wet BIG en art. 7:457 BW.

4 Zoals art. 8 EVRM, art. 12 UVRM, art. 17 IVBPR, art. 7 Handvest Grondrechten EU, art. 10 t/m 13 GW.

Het gegevensbeschermingsrecht is ontstaan in het kielzog van de snelle ontwikkeling van de informatietechnologie. In Nederland werd op 1 juli 1989 de Wet persoonsregistraties (Wpr) van kracht die in 2001 werd vervangen door de Wet bescherming persoonsgegevens (Wbp) en in 2018 door de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). Het Handvest van de Grondrechten van de EU dat in 2000 formeel werd aangenomen door het Europees Parlement, de Raad van de Europese Unie en de Europese Communie bevat in artikel 8 een specifiek grondrecht op bescherming van persoonsgegevens.

Naast het privacyrecht is het daarmee samenhangende gegevensbeschermingsrecht uitermate relevant in de gezondheidszorg. De digitalisering van zorgprocessen impliceert een onvermijdelijke sterke toename van verwerkingen van persoonsgegevens. Effectieve toegankelijkheid van het medisch dossier voor verschillende hulpverleners is belangrijk. Een betere informatiepositie vergroot de patiëntveiligheid en leidt ook tot meer doelmatigheid in de zorg. Gezondheidsgegevens worden vaker voor andere doeleinden gebruikt dan uitsluitend de individuele behandelrelatie, zoals kwaliteits- of onderzoeksdoeleinden. Tot slot wensen cliënten meer inzicht en controle.

Uitwisseling van persoonsgegevens is dus in de zorg in veel gevallen nuttig maar dient wel met voldoende waarborgen omkleed te zijn. Privacybescherming speelt een belangrijke rol bij het inperken van risico's die daarbij spelen.[5]

Gezondheidsgegevens vormen een bijzondere categorie persoonsgegevens. De verwerking daarvan is verboden tenzij een specifieke wettelijke uitzondering op dit verwerkingsverbod kan worden gevonden. De reikwijdte van de uitzonderingen is echter niet altijd even duidelijk. Daarnaast bevat het gegevensbeschermingsrecht aanvullende regels die gevolgen hebben voor de wijze waarop met gezondheidsgegevens dient te worden omgegaan. Het gaat bijvoorbeeld om beveiligingseisen, de plicht tot dataminimalisatie en rechten van betrokkenen.

Het vinden van de juiste balans tussen toegankelijkheid van gegevens en bescherming van privacy blijkt in wetgevingstrajecten én in de praktijk vaak een lastige opgave. Dat blijkt bijvoorbeeld uit de saga rond het landelijke Elektronisch Patiëntendossier. In 1996 werd het eerste initiatief genomen tot de ontwikkeling van zo'n EPD. In eerste instantie werd daarbij overwogen om met een chipcard te gaan werken met daarop per persoon het medisch dossier. Uiteindelijk sneuvelde het wetsvoorstel tot invoering van het landelijke EPD in 2011 in de Eerste Kamer wegens privacybezwaren. Vervolgens is een doorstart gemaakt met de 'zorginfrastructuur', het Landelijk Schakelpunt (LSP), onder verantwoordelijkheid van de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ). De rechtmatigheid van dit doorstartmodel werd echter ter discussie gesteld in een procedure tussen de Vereniging voor Praktijkhoudende Huisartsen (VPH) en de VZVZ die tot en met de Hoge Raad is gevoerd. De VZVZ trok aan het langste eind: het systeem werd in overeenstemming met het privacyrecht geacht. Daarbij werd echter wel de kanttekening gemaakt dat er naar gestreefd diende te worden om de toestemming die als grondslag voor de verwerking werd gebruikt in de toekomst specifieker te maken zodat een beter onderscheid gemaakt zou kunnen worden tussen (soorten) gegevens en (categorieën) zorgaanbieders. Dat streven was ook onderdeel van de Wet aanvullende bepalingen persoonsgegevens in de zorg (Wabvpz), maar lijkt wegens technische

5 O.a. H.J.J. Leenen e.a., *Handboek gezondheidsrecht*, Den Haag: Boom uitgevers 2020, p. 150.

onhaalbaarheid inmiddels definitief losgelaten.[6] Niet iedereen zal daardoor van mening zijn dat de juiste balans inmiddels is gevonden. Een alternatieve constructie wordt geboden met Mitz van het Programma Online Toestemmingsvoorziening. Ook die constructie is echter niet volledig vrij van kritiek.[7] Kortom, privacy in de zorg blijft altijd een heet hangijzer.

1.2 Opbouw

In Hoofdstuk 2, AVG en UAVG, wordt de AVG besproken en een overzicht gegeven van de belangrijkste begrippen uit het gegevensbeschermingsrecht. Aan de orde komen onder andere de actoren (verwerker en verwerkingsverantwoordelijke), de beginselen waar iedere verwerking van persoonsgegevens aan moet voldoen, verplichtingen van de verwerkingsverantwoordelijke en de rechten van betrokkenen.

Hoofdstuk 3 bevat een uitwerking van het beroepsgeheim en rechten van betrokkenen, de dossierplicht en de rechten van betrokkenen ten aanzien van de gegevensverwerking in het dossier. Uitgelegd wordt wanneer het medisch beroepsgeheim doorbroken kan worden. Een overzicht van gronden om het beroepsgeheim te mogen doorbreken en grondslagen en uitzonderingsgronden voor verwerking van (bijzondere) persoonsgegevens uit de AVG is te vinden in Bijlage 1.

Vervolgens wordt in Hoofdstuk 4 aandacht besteed aan de uitwisseling van gezondheidsgegevens bij samenwerking tussen zorgaanbieders. Het hoofdstuk bespreekt de verschillende manieren waarop gegevens kunnen worden uitgewisseld, landelijke ontwikkelingen ten aanzien van de registratie van toestemming voor gegevensuitwisseling en privacy vraagstukken die spelen bij samenwerking tussen zorgaanbieders.

Hoofdstuk 5 bespreekt de mogelijkheid om medische gegevens te gebruiken voor wetenschappelijk onderzoek. Daarbij wordt ingegaan op de Wet medisch-wetenschappelijk onderzoek (WMO) met mensen en de relevante artikelen uit de Wet op de geneeskundige behandelingsovereenkomst (Wgbo), tevens wordt de Gedragscode Gezondheidsonderzoek besproken.

In Hoofdstuk 6 wordt ingegaan op eHealth. De privacyrechtelijke aspecten van verschillende vormen van eHealth worden besproken: toepassingen gericht op patiënten zoals zelfhulp-apps en de persoonlijke gezondheidsomgeving, zorginformatiesystemen en professionele uitwisselingssystemen. Ook wordt stilgestaan bij medische hulpmiddelen, kunstmatige intelligentie en big data. Besproken wordt waar een gebruiker van eHealth-toepassingen bij stil moet staan alvorens een toepassing in gebruik te nemen.

Daarna wordt in Hoofdstuk 7 stilgestaan bij beveiliging. De AVG stelt algemene veiligheidseisen aan de verwerking van persoonsgegevens. In wetgeving op het gebied van de zorg worden echter specifieke aanvullende eisen gesteld die nader uitgewerkt zijn in NEN-normen. Besproken wordt hoe daaraan voldaan kan worden en dat naast technische beveiliging

6 Brief van de minister voor Medische Zorg en Sport van 2 oktober 2020, 1746657-210384-DICIO.

7 Zie bijvoorbeeld de inbreng van Privacy First op de Open Consultatie van het Informatieberaad Zorg voor de Online Toestemmingsvoorziening/Mitz, laatst geraadpleegd op 31-12-2021 op https://www.privacyfirst.nl/images/stories/medidossiers/SPF_20201005_02.pdf.