Juridische overwegingen bij medische data door MRDM en opslag bij Google Cloud

Op 1 april 2019 schreef ik op deze website een artikel over een bericht van het Algemeen Dagblad op 30 maart. Het betrof de verwerking van massale hoeveelheden medische data in gepseudonimiseerde vorm door het bedrijf Medical Research Data Management (MRDM) en de opslag van die data op de Google Cloud op de locatie Eemshaven. Inmiddels is de politiek ook wakker geschud, hebben Kamerleden van D66 en SP vragen gesteld en heeft minister Bruins opdracht gegeven aan de Autoriteit Persoonsgegevens onderzoek te doen. Er zitten interessante juridische kanten aan deze materie, voornamelijk van principiële aard. Niet alleen gaat het dan over het feit dat de data in de Google Cloud nu opgeslagen staan, maar ook over de positie van MRDM en de data-verzamelende zorginstellingen. De jurist Theo Hooghiemstra, kind aan huis bij het Ministerie van VWS, en in allerlei gremia betrokken bij data-uitwisseling, blijkt geen zwart/wit antwoord te kunnen geven of de in de Google Cloud opgeslagen data wel veilig zijn.

Onduidelijke positie MRDM

Uit de berichten in het Algemeen Dagblad doet het bedrijf MRDM voorkomen dat het contractueel een onderdeel is van de aanleverende zorginstellingen (zie daarin punt 4: Kan dit

zomaar?) en dus geen derde zou zijn die de data voor de zorginstellingen be-/verwerkt. Het bedrijf doet ermee voorkomen geen zelfstandige onderneming te zijn. Het vreemde aan die constructie is dat meerdere zorginstellingen dezelfde onderneming als onderdeel van hun organisatie zouden hebben. Dat maakt de zelfstandigheid van MDRM dan ook twijfelachtig. Toch profileert MRDM zich zelf naar buiten als een zelfstandige onderneming, als Trusted Party. Op haar website profileert MRDM zich ook als zelfstandige onderneming met **als klanten** een baaierd aan zorginstellingen.

Verwerkingsverantwoordelijke en be-/verwerker

Bij het be-/verwerken van data is er volgens de Algemene Verordening Gegevensbescherming(AVG) altijd een verwerkingsverantwoordelijke die het doel van en de middelen van de gegevensverwerking vaststelt. Deze heeft de zeggenschap over hetgeen wordt verwerkt, kan instructies geven voor de gegevensverwerking en heeft hierop feitelijke invloed. Het gaat hier vooral om wie daadwerkelijk de beslissingen neemt en feitelijk bepaalt wat er met die gegevens gebeurt. De verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. In het geval van gepseudonimiseerde zorgdata dienen we op basis van uitspraken van de Autoriteit Persoonsgegevens gewoon te spreken over het verwerken van (bijzondere) persoonsgegevens. Daarbij is bij hergebruik voor een ander doel toestemming van de patiënt noodzakelijk.

MRDM

De reactie van MRDM doet duidelijk uitkomen dat zij zichzelf “slechts” ziet als een bewerker die medische gegevens verwerkt in opdracht van ziekenhuizen. Dit standpunt houdt in dat MRDM niet eigenstandig mag beslissen op welke wijze en waarvoor de door ziekenhuizen aangeleverde data worden verwerkt. Dit

betekent ook dat de doorlevering van data aan Google gebeurt in opdracht van de ziekenhuizen die door MRDM worden aangemerkt als de verantwoordelijke voor de verwerkingen die door hen als bewerker worden uitgevoerd.

Eigen Initiatief?

Mocht de doorlevering van de medische data aan Google Cloud op eigen initiatief van MRDM geschied zijn dan moet zij worden aangemerkt als verwerkingsverantwoordelijke . Die kan en moet dan worden aangesproken op de vereisten die gelden voor het verwerken van deze bijzondere persoonsgegevens.

Wettelijke en verdragsrechtelijke eisen

Bewerkers die worden ingeschakeld voor de verwerking van bijzondere persoonsgegevens moeten gehouden kunnen worden aan dezelfde wettelijke en verdragsrechtelijke vereisten zoals die gelden voor de verwerkingsverantwoordelijke. Een andere opvatting is onhoudbaar omdat anders het inschakelen van een buitenlandse bewerker die niet gehouden is aan in Nederland geldige wet en regelgeving tot een “reguliere optie” wordt voor het in strijd met de wet(illegaal) verwerken van persoonsgegevens van Nederlanders.

Zeer problematisch

Een ander problematisch punt in deze casus is echter dat besturen van ziekenhuizen zonder toestemming van de patiënt menen te kunnen en mogen beschikken over behandelinformatie van in het ziekenhuis werkzame zorgverleners. De gegevens in dossiers van zorgverleners zijn verkregen voor de behandeling van de patiënt en mogen niet aan derden die niet direct bij de behandeling betrokken zijn slechts worden door geleverd voor enig ander welbepaald doel zonder expliciete geïnformeerde toestemming van de patiënt.

Toe-eigening zeggenschap zorgdata

Ook buiten deze casus speelt dit bij de pogingen tot verstrekking van ROM-data door GGZ-instellingen aan eerst SBG en thans Awka met De Nieuwe Entiteit als verwerker. De gedachte dat besturen van GGZ-instellingen uit hoofde van hun functie menen te kunnen beschikken over gegevens in patiëntdossiers van zorgverleners is volstrekt onjuist. In het model-privacy-reglement van GGZ Nederland voor GGZ-zorginstellingen worden de besturen van zorginstellingen tot verwerkingsverantwoordelijke gemaakt die het doel en de middelen van de verwerking vaststellen.

Het gevolg is dat niet de cliënt met de zorgverlener bepaalt of persoons-/behandelgegevens van de cliënt de instelling verlaten, maar de zorgaanbieder, zijnde het bestuur en de directie van de zorginstelling. Ik schreef hierover op 29 maart 2018.

Patiënten

Het is triest om te moeten constateren dat in dit data-geweld de rechten van patiënten om zelf te beschikken over wat er met zijn/haar data gebeurt met de voeten worden getreden. Allerlei constructies worden opgetuigd om over die data te beschikken. De Autoriteit Persoonsgegevens die daarover zouden moeten waken slaapt of is onwillig krachtige beslissingen te nemen.

W.J. Jongejan, 3 april 2019