Februari 2022

Speciale Zorg & ICT editie

Zorg in de praktijk

Digitaal uitwisselen van gegevens: dit zijn de speerpunten van de Wegiz

Wet AI in de zorg: nuttige aanvulling of lastig obstakel?

ZORG dat u bij bent in 2022

ICTRECHT
adviesbureau

ICTRecht: praktisch en deskundig

ICTRecht is hét grootste en meest ervaren fullservice adviesbureau op het gebied van ICT-recht, privacy en security. Met een team van meer dan 80 specialisten voorzien we onze klanten van deskundig en praktisch advies. Van startup tot multinational en van overheidsinstantie tot zorginstelling.

Wij zijn flexibel, innovatief en denken proactief met klanten mee. Onze adviezen zijn altijd concreet en begrijpelijk, en geven blijk van onze technische kennis.

Geen zes pagina's jargon met als conclusie "dat hangt ervan af", maar een duidelijk antwoord waarmee de organisatie direct aan de slag kan.

Hier zijn wij goed in:

ICT-recht - Privacy - Security - Legal tech - Academy - Detachering - Werving & selectie

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl

Index

Dit is een uitgave van ICTRecht B.V. Telefoonnummer: 020 663 1941, e-mail: info@ictrecht.nl.

Aan deze uitgave werkten mee:

Alexander Freund Information security consultant
a.freund@ictrecht.nl
Alisa Schurink Marketing adviseur
a.schurink@ictrecht.nl
Arnoud Engelfriet Algemeen directeur/ Opleidingsdirecteur
a.engelfriet@ictrecht.nl
Bram de Vos Juridisch adviseur
b.devos@ictrecht.nl
Britt Telleman Opleidingscoördinator
b.telleman@ictrecht.nl
Iris de Groot Juridisch adviseur
i.degroot@ictrecht.nl
Itte Overing Juridisch adviseur
i.overing@ictrecht.nl
Pelçim Kaygusuz Juridisch adviseur
p.kaygusuz@ictrecht.nl
Sanne Haumersen Juridisch adviseur
s.haumersen@ictrecht.nl
Sari Jansen Juridisch adviseur
s.jansen@ictrecht.nl
Tessa van Schijndel Juridisch adviseur
t.vanschijndel@ictrecht.nl
Amanda Butterworth Grafisch ontwerper
info@amandabutterworth.com
Leonard Fäustle Stills & Motion Foto's ICTRecht
info@leonardfaustle.nl

Itte Overing
Juridisch adviseur

Tessa van Schijndel
Juridisch adviseur

E-health Innovatie

Impact van de MDR op medische technologie in zorginstellingen

Als een zorginstelling een medisch hulpmiddel wil gebruiken, moet hij de kwaliteit van het hulpmiddel controleren om zo het verlenen van goede zorg te garanderen.[1] Het regelgevend kader waar men tot voor kort aan moest voldoen om een veilig hulpmiddel op de markt te brengen, stamde al uit 1994. Inmiddels hebben er veel nieuwe ontwikkelingen plaatsgevonden, waaronder de opkomst van medische technologie. Tijd voor een hoognodige update dus! De Europese Commissie heeft gesleuteld aan een nieuw regelgevend kader om de veiligheid van medische hulpmiddelen te garanderen. Sinds 26 mei 2021 is de Verordening medische hulpmiddelen (MDR) van toepassing. De MDR heeft niet alleen als doel om de veiligheid van medische hulpmiddelen te verbeteren, maar beoogt ook de prestaties van hulpmiddelen voor alle partijen inzichtelijker te maken. Ook is er een strenger regelgevend kader gecreëerd voor medische software.

Vrijwel iedereen in de zorg krijgt te maken met de nieuwe regels. Hoewel de MDR de meeste impact heeft op de fabrikanten[2] van medische hulpmiddelen, is er ook voor de zorginstelling een nieuwe rol weggelegd. Risicoklassen voor medische hulpmiddelen worden (vooral voor medische software) strenger en zorginstellingen kunnen ineens gezien worden als fabrikant. Daarnaast krijgen zorginstellingen een grotere rol in het garanderen van de veiligheid en kwaliteit van de medische hulpmiddelen. Afgelopen tijd zijn partijen druk bezig geweest met de implementatie van de nieuwe regels in de organi-

1. Artikel 4 Wet kwaliteit, klachten en geschillen zorg (Wkkgz) jo. artikel 4 uitvoeringsbesluit Wkkgz.
2. De fabrikant is degene die de hulpmiddelen onder zijn naam in de handel brengt.

satie. In de praktijk is gebleken dat niet iedereen de MDR op dezelfde wijze interpreteert. Beetje bij beetje wordt meer duidelijk over de wijze waarop de regels geïnterpreteerd moeten worden. In dit artikel zetten we de belangrijkste aandachtspunten voor zorginstellingen op een rij. En ICT-leveranciers: lees ook even mee. Het is altijd nuttig om te weten waar een zorginstelling tegenaan loopt bij de inkoop en het gebruik van medische hulpmiddelen.

Voor wie gelden de regels?

In de MDR zijn regels opgenomen voor fabrikanten, distributeurs en importeurs van medische hulpmiddelen. Afhankelijk van hoe de zorginstelling omgaat met medische hulpmiddelen, kan de zorginstelling (ook) als fabrikant, distributeur of importeur kwalificeren. Grofweg maken we een onderscheid tussen zorginstellingen die medische hulpmiddelen inkopen of (intern) ontwikkelen.

Kwalificatie en risicoclassificatie

Een hulpmiddel (waaronder software) die door de fabrikant bedoeld is om te worden gebruikt voor een medisch doeleinde, zoals voor het diagnosticeren, voorspellen, het stellen van een diagnose of behandelen van een ziekte, letsel of een beperking wordt onder de MDR aangemerkt als een medisch hulpmiddel.[3]

3. Artikel 2 onder 12 jo. artikel 2 onder 36 MDR (EU) 745/2017.

Software dat niet gebruikt wordt voor een individuele patiënt of voor enkel opslag, archivering of het reconstrueren van data, wordt niet beschouwd als een medisch hulpmiddel. Ook software die als communicatiemiddel wordt gebruikt of software die simpele zoekopdrachten uitvoert, valt niet onder de definitie van een medisch hulpmiddel.

Het kwalificeren en classificeren van medische hulpmiddelen is niet alleen een taak van de fabrikant. Voor het verlenen van goede zorg mogen zorginstellingen alleen maar medische hulpmiddelen gebruiken die een CE-markering hebben. Om dit te controleren moeten zorginstellingen zelf in kaart brengen welk hulpmiddel een medisch hulpmiddel in de zin van de MDR is en in welke risicoklasse het hulpmiddel valt.

Controleer de beschikbaarheid van de medische hulpmiddelen

Door de aangescherpte wetgeving wordt (steeds meer) software als een medisch hulpmiddel aangemerkt, valt de software in een hogere risicoklasse en zijn fabrikanten verplicht om aan strengere verplichtingen te voldoen, zoals een beoordeling door een externe partij. Deze veranderingen kunnen gevolgen hebben voor de beschikbaarheid van medische hulpmiddelen voor zorginstellingen. Fabrikanten kunnen hun medische software aanpassen, zodat zij niet onder de MDR vallen of besluiten om de ontwikkeling van medische software te staken. Bovendien is het mogelijk dat bepaalde medische hulpmiddelen waarvoor niet op tijd certificaten worden verkregen, tijdelijk niet beschikbaar zullen zijn.

Medische hulpmiddelen die niet voorzien zijn van een CE-markering mogen niet meer worden gebruikt. Hiervoor geldt echter wel een uitzondering. Fabrikanten kunnen onder omstandigheden gebruikmaken van het overgangsrecht. Hierdoor kan het hulpmiddel tot 26 mei 2024 onder de oude wetgeving nog worden verkocht en gekocht, mits er geen (significante) wijzigingen aan het hulpmiddel worden aangebracht. Het gaat dan om een significante wijziging van het design van de medische software of van het beoogd doel van de software.[4]

4. https://bit.ly/3JnRlSO.

Regels bij inkoop van medische hulpmiddelen

Bij de inkoop en het beheer van medische hulpmiddelen gelden er voor de zorginstelling de volgende verplichtingen:

- Opvolgen van instructies van de fabrikant: zorginstellingen moeten bij het gebruik van een hulpmiddel alle instructies van de fabrikant opvolgen. Niet alleen over het gebruik van het hulpmiddel, maar ook ten aanzien van het doorvoeren van updates en ander onderhoud dat verricht moet worden. Worden de instructies niet opgevolgd, dan loopt de zorginstelling het risico om als fabrikant te worden aangemerkt.
- Meewerken aan post-market surveillance: zorginstellingen moeten fabrikanten van informatie voorzien in het kader van de post-market surveillance. Fabrikanten hebben onder andere informatie nodig over gebruikerservaringen, updates, storingen, datalekken, cyberaanvallen en andere incidenten die zich hebben voorgedaan met het hulpmiddel.

- Melden van incidenten: zorginstellingen moeten incidenten melden bij het toezichthoudende orgaan, de Inspectie Gezondheidszorg en Jeugd (IGJ). Via een Algemene Maatregel van Bestuur (AMvB) zal er een nadere invulling aan deze meldplicht worden gegeven.
- Controle in EUDAMED: zorginstellingen moeten bij de inkoop en daarna periodiek controleren of het hulpmiddel nog over een geldige CE-markering beschikt. De zorginstellingen kunnen de geldigheid van het CE-certificaat controleren in de EUDAMED (European database on medical devices). Fabrikanten moeten gegevens van het hulpmiddel en de UDI (unique identification number) opnemen in de EUDAMED.

Intern vervaardigde hulpmiddelen moeten ook aan de MDR voldoen

Onder de MDR mogen medische hulpmiddelen alleen nog worden gebruikt in lijn met het beoogde doel van de fabrikant. Voor dat beoogde doel heeft de fabrikant een CE-markering verkregen en ander gebruik is verboden. Indien er geen geschikt medisch hulpmiddel op de markt is, of indien het aangeboden hulpmiddel de CE-markering mist, dan kunnen zorginstellingen overwegen om zelf een medisch hulpmiddel te ontwikkelen voor een eigen beoogd doel. Ook biedt de MDR de mogelijkheid om een medisch hulpmiddel van een fabrikant te wijzigen of voor een ander doel in te zetten, maar dan moet de zorginstelling de verplichtingen van de fabrikant op zich nemen.

De intern vervaardigde of gewijzigde hulpmiddelen voldoen aan de algemene vereisten voor veiligheid en prestatie in Annex I van de MDR. Afwijkingen hiervan moeten worden onderbouwd. Daarnaast moet de zorginstelling het ontwerp adequaat documenteren in een technisch dossier, over een passend kwaliteitssysteem en risicomanagementsysteem beschikken en klinische evaluaties uitvoeren. Ook hier zal de IGJ toezicht op gaan houden. De IGJ kan steekproefsgewijs documentatie opvragen ter controle.

Als de zorginstelling wel besluit om het hulpmiddel over te dragen aan een andere rechtspersoon, dan zal zij moeten voldoen aan de verplichtingen die gelden voor fabrikanten. Denk aan de beoordeling van het hulpmiddel door de *notified body* en het aanstellen van een persoon die verantwoordelijk is voor de naleving van de MDR (PRRC).

De zorginstelling kwalificeert zich echter als zij het hulpmiddel verhandelen, ongeacht of dit tegen betaling is. Let op: deze eisen zijn erg streng! Zelfs als het hulpmiddel gratis aan een andere entiteit ter beschikking wordt gesteld, wordt de instelling aangemerkt als fabrikant.[5]

5. Artikel 5 lid 5 MDR (EU) 745/2017.

Plan van aanpak

Voldoet u al aan de MDR? Of moet u nog beginnen? Als zorginstelling moet je in beeld hebben wat de MDR betekent voor het verlenen van goede zorg. Om dit in kaart te brengen, bevat een gedegen plan van aanpak in ieder geval een nulmeting, gap-analyse en een roadmap.

Tijdens de nulmeting beoordeelt u de reeds ingekochte medische hulpmiddelen, stelt u de stand van zaken vast met betrekking tot intern vervaardigde hulpmiddelen en beoordeelt u aan welke verplichtingen u al wel voldoet en welke nog niet. Het is goed mogelijk dat u al aan bepaalde verplichtingen uit de MDR voldoet door de overlap met andere wetgeving, zoals de Algemene verordening gegevensbescherming (AVG) en de Wkkgz. Hierna kan er doormiddel van een roadmap in kaart worden gebracht welke maatregelen er nog genomen moeten worden om te voldoen aan de MDR om ten slotte aan de slag te gaan met de implementatie. In veel gevallen moet u ook een kwaliteitsmanagementsysteem implementeren. Dergelijk systeem kent de plan-do-check-act cyclus. Na de implementatie is dus beheer nodig van de getroffen maatregelen, na de “do”-fase komt u (na verloop van tijd) in de check-fase. Wellicht heeft u deze cyclus reeds in uw bedrijfsvoering geïmplementeerd, de maatregelen ten behoeve van het veilig gebruik maken (en doorontwikkeling indien relevant) van medische hulpmiddelen moeten hierin worden meegenomen.

26 mei 2021 is verstreken. De MDR is van toepassing. De deadline zal niet meer opschuiven. Na een jaar vertraging als gevolg van de coronapandemie kunnen betrokken partijen niet langer meer wachten. De MDR is van toepassing en die zal worden gehandhaafd. Dit vergt ook voor zorginstellingen een goede voorbereiding, want de MDR bevat harde sancties.

Brengt u medische software op de markt?

ICTRECHT adviesbureau

Vanaf 26 mei 2021 geldt de nieuwe wetgeving over medische hulpmiddelen: de Medical Device Regulation (MDR). Brengt u software met een medisch doeleinde op de markt? Wellicht levert u dan een medisch hulpmiddel. Afhankelijk van de risico's die de medische software met zich meebrengt, wordt het medisch hulpmiddel in een bepaalde risicoklasse ingedeeld. Wanneer niet wordt voldaan aan de MDR, kunnen er boetes worden opgelegd (tot € 870.000 of 10% van de omzet van het laatste boekjaar).

ICTRecht biedt MDR-specialisten aan met kennis van regelgeving en kwaliteitsmanagementsystemen voor medische hulpmiddelen die u kunnen helpen met:

- het kwalificeren en classificeren van medische software;
- het bieden van ondersteuning bij de voorbereiding op de conformiteitsbeoordeling door een *notified body*;
- het vervullen van de rol van een "Person Responsible for Regulatory Compliance" (PRRC) op afstand of op locatie;
- het opleiden van uw eigen PRRC.

Meer weten?
Lees onze factsheet op: ictrecht.nl/factsheet-MDR
Of neem contact op via: zorg@ictrecht.nl

Sari Jansen
Juridisch adviseur

E-health Privacy Security

Digitaal uitwisselen van gegevens: dit zijn de speerpunten van de Wegiz

NEN 7510, NEN 7512 en NEN 7513. Zo langzamerhand de verplichte kost voor elke zorgaanbieder en haar ICT-leverancier als het gaat om informatieveiligheid. NEN 7510 wordt al sinds 2013 door de Autoriteit Persoonsgegevens, toen nog CBP, genoemd als de gangbare standaard voor passende (organisatorische) beveiliging. Sinds 2018 is de zorgaanbieder ook verplicht om bij het gebruik van een zorginformatiesysteem of elektronisch uitwisselingssysteem te voldoen aan de genoemde NEN-normen.[1] Standaardisatie is ook nodig om de tijdigheid en kwaliteit van zorg te borgen.

1. Op grond van het Besluit elektronische gegevensverwerking door zorgaanbieders.

Doordat zorgaanbieders veelal zijn aangesloten op verschillende systemen, is echter niet altijd de juiste informatie voor de zorgverlening tijdig beschikbaar. Het Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg (Wegiz) regelt dat specifieke gegevensuitwisselingen tussen zorgverleners verplicht elektronisch gaan verlopen. In dit artikel bespreken we de speerpunten van het voorliggende wetsvoorstel en de huidige stand van zaken.

Interopabiliteit

Eén van de speerpunten van de Wegiz is het creëren van optimale interoperabiliteit tussen de verschillende gebruikte systemen. Door het veld zijn al

stappen gezet naar het realiseren van gestandaardiseerde elektronische gegevensuitwisseling (denk aan standaarden zoals HL7[2]). Desondanks zijn de problemen door het gebrek aan eenduidige taal, techniek en regie nog niet opgelost.

2. www.nictiz.nl/overzicht-standaarden.

Standaardisatie

Met het wetsvoorstel worden zorgaanbieders stapsgewijs verplicht om erop toe te zien dat ze gegevens onderling tenminste elektronisch met elkaar uitwisselen. De bedoeling is dat dit uiteindelijk gestandaardiseerd plaatsvindt. Het idee is om per gegevensuitwisseling een standaard te formaliseren die (uiteindelijk) in een Algemene Maatregel van Bestuur (AMvB) wordt vastgelegd. Waar mogelijk, spoor 1, wordt het aan het veld overgelaten om de standaard vorm te geven in samenwerking met het Nederlandse normalisatie instituut (NEN). Indien of voor zover dat niet lukt, spoor 2, kan een standaard middels AMvB worden afgedwongen. Hiermee wordt interoperabiliteit geborgd.

Vijf lagen van interoperabiliteit

Om optimale interoperabiliteit te creëren, moet er echter op meerdere niveaus maatregelen genomen worden. Het Nederlandse kenniscentrum voor landelijke toepassingen in de zorg Nictiz onderscheidt daarom vijf lagen van interoperabiliteit.[3] De standaarden en normen zullen deze vijf lagen van interoperabiliteit moeten invullen. Uit het model blijkt dat er niet alleen maatregelen moeten worden getroffen op het niveau van techniek (infrastructuur en applicatie), maar ook op het niveau van informatieaspecten; in het zorgproces en op organisatieniveau.

3. www.nictiz.nl/standaardisatie/interoperabiliteit.

Voorbeelden van standaarden op het niveau van het zorgproces (tweede laag) zijn de Zorgstandaard COPD en Richtlijn Overdracht van medicatiegegevens in de Keten. Voorbeelden op het niveau van informatie (de derde laag) zijn terminologiestandaarden, classificaties en informatiestandaarden zoals SNOMED, ICF en Huisartswaarneming. Op applicatieniveau (vierde laag) kan gedacht worden aan HL7, FHIR en EDIFACT. Bij de laatste laag, welke betrekking heeft op de technische infrastructuur, kan men denken aan standaarden als LSP, IHE en XDS.

Uitwerking in AMvB's

In de AMvB's zal verwezen worden naar normen waarin de te gebruiken standaarden voor de gegevensuitwisseling worden gespecificeerd. Voor wat betreft de eisen aan taal en techniek zullen dit uitsluitend NEN-normen zijn (spoor 2). Daarbij is het de intentie dat de standaard op een bestendige wijze in de NEN-norm wordt opgenomen, zodat niet elke nieuwe versie van de standaard een nieuwe NEN-norm tot gevolg heeft. Hoe dit er concreet zal uit komen te zien, zal moeten blijken. Het is voor te stellen is dat er naar de vindplaats van een bepaalde standaard zal worden verwezen, in plaats van naar een specifieke versie. De minister verwacht dat de eerste AMvB in 2026 een wettelijke verplichting zal worden.

In de NEN-normen worden zowel de eisen opgenomen waaraan de zorgaanbieder moet voldoen, als de eisen waaraan het product of de dienst moet voldoen. Denk aan NEN 7510 (informatiebeveiliging), NEN 7512 (vertrouwensbasis voor gegevensuitwisseling) en NEN 7513 (logging). Voor zover deze normen dat nog niet zijn, zullen ze verplichte kost worden voor de zorgaanbieder en haar ICT-leverancier.

Ontwikkeling van normen en certificatieschema's

NEN ontwikkelt in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) en samen met het zorgveld een uitgebreid stelsel van normen en certificatieschema's die het fundament zijn voor de elektronische gegevensuitwisseling. Eind 2019 is NEN gestart met de herziening van de norm met eisen voor digitaal receptenverkeer dat na actualisatie het medicatieproces ondersteunt (NEN 7503). Het receptenverkeer zal als eerste aan de beurt komen als verplichte gegevensuitwisseling onder de Wegiz. In de herziene versie van NEN 7503 zullen ook nieuwe eisen worden opgenomen om de interoperabiliteit beter te borgen.

Gevolgen voor ICT-leveranciers

ICT-leveranciers zullen extra werk moeten verzetten en kosten moeten maken om aan de eisen voor interoperabiliteit te kunnen voldoen. Denk aan de initiële investering om de diensten aan te passen en te certificeren, maar ook aan kosten voor periodieke hercertificering en controles. Omdat de NEN-normen enkel voor de Nederlandse markt gelden, wordt een negatief effect verwacht voor ICT-leveranciers die een internationale markt bedienen. Zij zullen maatwerkoplossingen moeten ontwikkelen voor de Ne-

“Naast het creëren van optimale interopabiliteit, is het borgen van keuzevrijheid een belangrijk speerpunt van de Wegiz. Gestandaardiseerde gegevensuitwisseling zou (onder andere) moeten leiden tot meer openheid en een vermindering van de sterke marktpositie van grote ICT-leveranciers.”

Sari Jansen
Juridisch adviseur

derlandse markt en zullen daarom mogelijk de keuze maken hun producten niet meer op de Nederlandse markt aan te bieden. Volgens de minister staat daar onder andere wel tegenover dat de standaardisatie de marktwerking en transparantie zal bevorderen.

Keuzevrijheid

Naast het creëren van optimale interopabiliteit, is het borgen van keuzevrijheid een belangrijk speerpunt van de Wegiz. Gestandaardiseerde gegevensuitwisseling zou (onder andere) moeten leiden tot meer openheid en een vermindering van de sterke marktpositie van grote ICT-leveranciers. Voor systemen die de aangewezen gegevensuitwisselingen ondersteunen geldt een certificatieplicht. Door de verplichte certificering van systemen voor elektronische gegevensuitwisseling kunnen zorgaanbieders erop vertrouwen dat deze systemen aan de gestelde eisen voldoen. Zorgaanbieders kunnen dan zelf besluiten van welke infrastructuur ze gebruik maken bij het uitwisselen, zolang men zich aan de standaard voor techniek, taal en inhoud, houdt. De zorgaanbieder hoeft niet te voldoen aan de (technische) eisen die bij of krachtens AMvB zijn gesteld, wel is het aan haar om alleen gebruik te maken van gecertificeerde producten (als een certificaat verplicht is gesteld). Hiermee worden ook ICT-leveranciers (indirect) gebonden aan de Wegiz.

Privacyrechtelijke grondslag

Bij de Wegiz staat de uitwisseling van bijzondere persoonsgegevens (gezondheidsgegevens) van patiënten centraal. Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij een uitzonderingsgrond uit de Algemene verordening gegevensbescherming (AVG) van toepassing is. Is het verbod doorbroken, dan is er ook een rechtsgeldige grondslag nodig om persoonsgegevens te verwerken. Dat betekent dat de eerste stap dus altijd is om te toetsen of het verwerkingsverbod uit de AVG doorbroken kan worden, of er vervolgens een grondslag aanwezig is, en of het medisch beroepsgeheim doorbroken kan worden.

Een interessant aspect is dat de patiënt op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg uitdrukkelijk toestemming dient te geven voor het beschikbaar stellen van gegevens via een elektronisch uitwisselingssysteem. Bij het Landelijk Schakelpunt (LSP) dienen patiënten bijvoorbeeld uitdrukkelijke toestemming te geven, zodat de huisarts en de apotheek het BSN aan kunnen melden bij de verwijsindex. Andere zorgaanbieders kunnen hiermee zien welke zorgaanbieders welke gezondheidsgegevens delen. Het gaat hierbij om toestemming voor het gebruik van het systeem, niet om de uitwisseling an sich. Dit kan tot de situatie leiden dat gegevens uitgewisseld mogen worden (het verwerkingsverbod is doorbroken en er is een grondslag), dat dit elektronisch dient te verlopen op grond van de Wegiz, maar dat er geen toestemming is voor het gebruik van het elektronisch uitwisselingssysteem. In dit geval zal de uitwisseling op een andere manier elektronisch moeten plaatsvinden dan via het systeem waar toestemming voor nodig is.

Huidige stand van zaken

De Wegiz is afgelopen 3 mei aangeboden aan de Tweede Kamer.[4] Vanuit de Kamer zijn er vervolgens meer dan 350 vragen gesteld over het wetsvoorstel. De vragen die de Kamer in juni stelde gaan onder andere over de verhouding met andere wetten, de bekostiging van de implementatie, en het draagvlak van de wet in het zorgveld. Maar ook over wat de patiënt ervan gaat merken, en hoe de Wegiz aansluit op ontwikkelingen in de Europese Unie en daarbuiten. De beantwoording van de vragen is uiteengezet in het verslag dat de Kamer afgelopen 18 oktober heeft ontvangen.[5] Daarnaast heeft de Kamer een Kamerbrief van de minister gekregen waarin hij onder meer ingaat op de stappen die reeds zijn gezet en welke nog genomen worden.[6]

4. https://bit.ly/3p66FeK.
5. https://bit.ly/3E3f1bf.
6. https://bit.ly/3GXDArV.

In die brief beschrijft de minister ook een aantal belangrijke onderwerpen uit de beantwoording van de schriftelijke behandeling van de Wegiz. Een vaak terugkomende vraag ziet op het karakter van de Wegiz, en met name de vraag of het wetsvoorstel verplicht tot het uitwisselen van gegevens en daarmee het mogelijk breken van het beroepsgeheim. De minister schrijft dat het wetsvoorstel nadrukkelijk niet verplicht tot het uitwisselen van gegevens. Het doel van en de grondslag voor de verwerking van persoonsgegevens worden bepaald in andere regelgeving. De verplichting ziet alleen op het hoe van de uitwisseling, namelijk op elektronische wijze. Dat er geen verplichting is tot uitwisseling, is nu ook expliciet in de tekst van de Wegiz

opgenomen.[7] Dat is overigens ook meteen de enige wijziging van de wettekst naar aanleiding van alle vragen.

7. Zie voor de nota van wijziging: https://bit.ly/32eyTez.

In de Kamerbrief beschrijft de minister, naast het bovenstaande, hoe hij zijn regierol wil invullen binnen het stelsel van de zorg-ICT. Daarbij zijn de randvoorwaarden voor uitwisseling een belangrijk thema. In dit kader is onder meer advies uitgevraagd en ontvangen ten aanzien van het houderschap van informatiestandaarden. Met houderschap wordt het beheren en doorontwikkelen van de informatiestandaarden bedoeld.

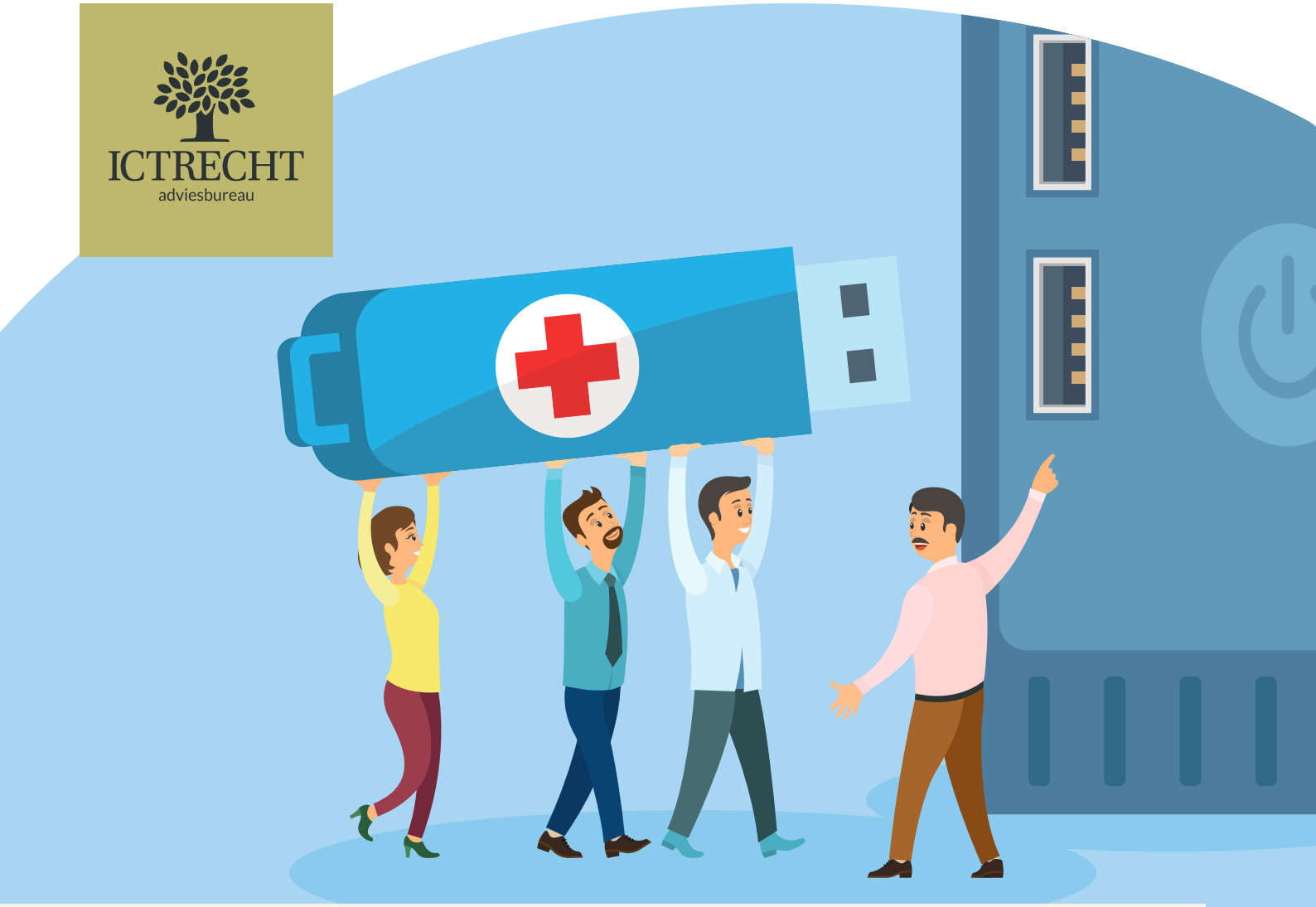
Kortgezegd wordt geadviseerd om het houderschap en voor een termijn van maximaal drie jaar onder te brengen bij een regie-organisatie waarin het veld en het ministerie van VWS vertegenwoordigd zijn en samen wordt gewerkt op basis van een convenant. Zo kan de minister erop toezien dat normen onder de Wegiz aansluiten op afsprakenstelsels zoals MedMij, wat belangrijk is voor het ontsluiten in Persoonlijke Gezondheidsomgevingen (PGO's). De minister heeft een kwartiermaker aangesteld om te onderzoeken of de inrichting die wordt geadviseerd wenselijk en noodzakelijk is. De resultaten worden begin volgend jaar verwacht.

Daarnaast zal er meer regie worden genomen op een landelijk dekkend stelsel van infrastructuur, generieke functies en aanpalende ICT-voorzieningen. Over het reeds bestaande LSP zegt de minister (in het verslag) dat deze net als ieder ander informatietechnologieproduct of –dienst die of dat gebruikt wordt in een aangewezen gegevensuitwisseling, moet voldoen aan de eisen die gesteld worden onder het wetsvoorstel. De minister onderzoekt op welke wijze dit het beste vorm kan krijgen. Daarbij kan gedacht worden aan eisen aan toegang tot gegevens in systemen, zoals open API's, of eisen aan interopabiliteit tussen (delen van) infrastructuren, zoals NTA7516 voor veilig mailverkeer. Daarnaast wordt er gewerkt aan een opvolger van de UZI-pas en is een voorziening ontwikkeld waarmee zorginstellingen via inlogmiddelen zoals DigiD hun digitale dienstverlening kunnen ontsluiten (ToegangsVerleningService).

Ook wordt op dit moment onderzocht welke problemen bestaan rondom het verlenen van toestemming voor gegevensverwerking in de zorg. Daarbij wordt gekeken of de wettelijke grondslagen voor gegevensverwerking nog in lijn zijn met de omslag van papier naar digitaal. De minister geeft aan dat de toestemmingsvoorziening Mitz onder strenge voorwaarden al op DigiD mag aansluiten. Onderwerpen als informatieveiligheid, de slimme inzet van kunstmatige intelligentie in de zorg, hergebruik van gegevens en grensoverschrijdende gegevensuitwisseling passeren daarnaast ook nog de revue in de brief.

Nu de Kamer antwoorden op de ruim 350 vragen heeft ontvangen, is de verwachting dat de Kamer begin volgend jaar het wetsvoorstel plenair zal behandelen. Naar verwachting zal de eerste gegevensuitwisseling, als het wetsvoorstel wordt aangenomen, dan in 2023 in werking treden. Bent u er al klaar voor?

ICTRECHT
adviesbureau



Wisselt u elektronisch patiëntgegevens uit?

Het uitwisselen van medische gegevens tussen zorgaanbieders kan en moet steeds vaker elektronisch. Dit kan via een elektronisch uitwisselingssysteem, maar ook via een ander systeem dat ingericht is voor het uitwisselen van medische gegevens. Bij het uitwisselen van medische persoonsgegevens geldt diverse regelgeving. ICTRecht helpt uw organisatie om deze regelgeving te vertalen naar de praktijk.

Onze ondersteuning kan onder andere bestaan uit:

- **Het adviseren over hoe u kunt voldoen aan wet- en regelgeving**
- **Het opstellen of beoordelen van documenten**
- **Het doen van onderhandelingen**
- **Het leveren van continue ondersteuning op afstand of op locatie**

Meer weten?

Ga naar: ictrecht.nl/elektronisch-uitwisselen-medische-gegevens
Of neem contact op via: zorg@ictrecht.nl

Pelçim Kaygusuz
Juridisch adviseur

Bram de Vos
Juridisch adviseur

E-health Innovatie

Wet AI in de zorg: nuttige aanvulling of lastig obstakel?

"Artificiële Intelligentie (AI) is niet zomaar een technologie, maar een systeemtechnologie die de samenleving fundamenteel zal veranderen." Zo opende de Wetenschappelijke Raad voor het Regeringsbeleid een recent adviesrapport over AI en publieke waarden.[1] Al sinds de jaren 50 van de vorige eeuw wordt er in de wetenschap geëxperimenteerd met technieken om computers 'intelligent' en 'autonoom' te maken. Maar naarmate de computers krachtiger worden en er steeds grotere datasets beschikbaar komen, zien we AI ook steeds vaker toegepast in de wereld om ons heen. Denk aan de automotive industrie (de zelfrijdende auto), de financiële sector (de robotbelegger) maar óók aan de zorgsector waarin steeds vaker gebruik wordt gemaakt van AI.

De toepassing van AI in de zorg biedt enorme kansen. Door bijvoorbeeld een AI in te zetten om testuitslagen te helpen beoordelen, kan de kans op verkeerde diagnoses worden verkleind.[2] Of denk aan de inzet van slimme chatbots: wellicht kan men op deze manier de triage verbeteren en daarmee indirect de druk op de zorg verminderen.[3] Maar aan dergelijke toepassingen kleven vanzelfsprekend ook (significante risico's. We zijn het afgelopen jaar ondergesneeuwd met mediaberichten over tekorten in de zorg. Wat als een arts om tijd te besparen te veel op zijn AI-hulpje vertrouwt waardoor onverhoopt een verkeerde diagnose wordt gesteld? En willen we de triage überhaupt wel uitbesteden aan een robot? "Goede dokters kennen alle protocollen, slechte dokters voeren ze uit" ving ik onlangs op. Worden we niet veel te afhankelijk van vastomlijnde procedures en regeltjes wanneer we dergelijke zorgtaken bij een AI neerleggen?

Ook de wetgever is zich wel degelijk van de hiervoor aangehaalde risico's bewust. Onlangs presenteerde de Europese Commissie daarom een voorstel voor een Wet op de artificiële intelligentie (Wet AI).[4] Met dit voorstel hoopt men de risico's die kleven aan AI beter

beheersbaar te maken. Niet alleen in de zorg, maar in álle domeinen waarin AI kan worden ingezet. Een complicerende factor is daarbij dat we voor de toepassing van AI in de zorg al een uitgebreid regelgevend kader hebben. Een AI-zorgsysteem kan namelijk al snel worden aangemerkt als medisch hulpmiddel. Daarmee valt het systeem automatisch onder de Verordening medische hulpmiddelen (MDR).[5] Qua opzet en insteek zijn er duidelijke paralellen tussen de nu voorgestelde Wet AI en de MDR. Daarmee rijst ook de vraag: hoe verhoudt het een zich tot het ander? En zijn deze wetgevingsinstrumenten wel verenigbaar met elkaar?

Achtergrond Wet AI

AI in 2018 bestempelde de Europese Commissie AI als één van haar beleidsspeerpunten. Dit heeft onder meer geresulteerd in een aantal resoluties van het Europees Parlement.[6] Dergelijke resoluties bevatten geen concrete regelgeving, maar zijn bedoeld om de Europese Unie in actie te laten komen. Met het voorstel voor de Wet AI is er nu een eerste aanzet voor daadwerkelijke en dwingende spelregels. De Wet AI moet overigens nog wel door de Europese wetgevingsprocedure worden geloodst. Dat betekent ook dat er nog inhoudelijke wijzigingen in het voorstel kunnen worden doorgevoerd. Voor dit artikel gaan wij echter uit van het voorstel zoals dat nu door de Europese Commissie is gepresenteerd.

1. *Opgave AI. De nieuwe systeemtechnologie* (WRR-adviesrapport in opdracht van het kabinet), Den Haag: 11 november 2021, zie ook wrr.nl.
2. Een mooi voorbeeld hiervan is het bedrijf PathAI, dat gebruik maakt van AI om pathologen te ondersteunen bij het beoordelen van lichaamsweefsel, zie ook pathai.com.
3. Denk bijvoorbeeld Buoy Health, een bedrijf dat AI-chatbots ontwikkelt die zelfstandig symptomen van patiënten kunnen uitvragen en beoordelen, zie ook buoyhealth.com.
4. Voorstel voor een Verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Wet op de artificiële intelligentie).
5. Verordening van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen (Verordening medische hulpmiddelen).
6. Zie onder meer het Ontwerpverslag van het Europees Parlement, kunstmatige intelligentie in het strafrecht en het gebruik ervan door politie en justitie in strafzaken, 2020/2016 en het Ontwerpverslag van het Europees Parlement, kunstmatige intelligentie in onderwijs, cultuur en de audiovisuele sector, 2020/2017.

“De Wet AI moet een juridisch kader gaan bieden voor alle soorten AI-toepassingen, zolang er een directe of indirecte relatie is met de Europese Unie.”

Pelçim Kaygusuz
Juridisch adviseur

Bram de Vos
Juridisch adviseur

Toepassingsbereik en opzet Wet AI

De Wet AI moet een juridisch kader gaan bieden voor alle soorten AI-toepassingen, zolang er een directe of indirecte relatie is met de Europese Unie.[7] Dat kan doordat de AI in de handel wordt gebracht of in gebruik wordt gesteld binnen de Europese Unie, maar ook doordat de gebruikers van de AI-toepassing zich in Europa bevinden. Zelfs als de aanbieders én de gebruikers zich buiten Europa bevinden, maar de ‘output’ van de AI in Europa wordt gebruikt, is de Wet AI van toepassing.[8]

7. Zie ook bijlage I bij de Wet AI, waaruit blijkt dat zowel ‘machine learning’ als verdergaande AI-toepassingen (ook wel aangeduid als ‘expert systems’) onder het toepassingsbereik vallen. Daarnaast volgt uit overweging 6 bij de Wet AI dat de definitie tussentijds kan worden bijgesteld als dit in verband met nieuwe technologieën of marktontwikkelingen nodig is.
8. Zie ook artikel 2 van de Wet AI.

De Wet AI gaat uit van een risico-georiënteerde benadering. Afhankelijk van de toepassing kunnen er zwaardere of juist mildere verplichtingen gelden. Daarbij kan onderscheid gemaakt worden tussen de volgende categorieën:

1. **Verboden toepassingen:** sommige toepassingen brengen onaanvaardbare risico’s met zich mee, bijvoorbeeld omdat deze een schending van grondrechten opleveren. Het gaat dan onder meer om AI-toepassingen die bestemd zijn om mensen te manipuleren of uit te buiten. Maar denk ook aan ‘social scoring’ van burgers door de overheid. De Wet AI bevat een limitatieve lijst van dit soort verboden AI-toepassingen die tussentijds kan worden aangepast.[9]
2. **Toepassingen met een hoog risico:** het gaat hier om toepassingen die substantiële risico’s voor de gezondheid, veiligheid of grondrechten van natuurlijke personen meebrengen. Een aantal van dit soort toepassingen wordt expliciet genoemd in bijlage III bij het voorstel voor de Wet AI. Daarnaast worden AI-toepassingen die al aan sectorspecifieke regels voor productveiligheid zijn onderworpen bestempeld als hoog risico toepassing. Dit geldt echter alleen als onder die sectorspecifieke regels een conformiteitsbeoordeling door een derde partij vereist is.[10] In bijlage II bij de Wet AI wordt uitgewerkt om welke sectorspecifieke regels het gaat. Daarin wordt óók de MDR genoemd. Daarmee zullen AI-toepassingen die als medisch hulpmiddel kwalificeren meestal een hoog risico toepassing zijn.[11]

9. Zie bijlage I bij de Wet AI.
10. Zie ook artikel 6 van de Wet AI.
11. De MDR stelt in de meeste gevallen een conformiteitsbeoordeling door een ‘notified body’ verplicht. In de praktijk zullen alle AI-toepassingen die onder de MDR in klasse IIa of hoger vallen, als hoog risico toepassing moeten worden aangemerkt.

3. **AI-systemen met verwarringsgevaar:** er is een bijzondere plaats gereserveerd voor AI-systemen waarmee verwarringsgevaar gepaard gaat. Daarbij kan bijvoorbeeld gedacht worden aan chatbots of AI-toepassingen waarmee 'deep fakes' kunnen worden gemaakt. Om te voorkomen dat mensen niet doorhebben dat zij met een computer te maken hebben, gelden voor dit soort AI-toepassingen transparantieverplichtingen.[12]
4. **Toepassingen met een laag risico:** hieronder vallen toepassingen die geen of slechts beperkte gevolgen hebben voor de gezondheid, veiligheid en grondrechten van natuurlijke personen. Onder deze categorie vallen bijvoorbeeld spamfilters die gebruik maken van AI om ongewenste e-mail te herkennen. Gelet op de beperkte risico's mogen deze AI-systemen worden ingezet zonder aan verdere eisen te voldoen.[13]

12. Zie hierover ook titel IV van de Wet AI.
13. Aanbieders worden wel aangemoedigd om gedragscodes op te stellen. Zie ook overweging 81 bij de Wet AI.

Samenloop Wet AI en MDR

Zoals in de vorige sectie al kort werd aangestipt, vallen AI-toepassingen die als medisch hulpmiddel kwalificeren meestal in de hoog risico categorie. Daarmee moeten zij ook aan de inhoudelijke eisen uit de Wet AI voldoen. Bij de beoordeling of een AI-toepassing kwalificeert als medisch hulpmiddel is de kernvraag of deze bestemd is voor medische doeleinden.[14] Daarbij moet onder andere worden gedacht aan de diagnose, preventie, monitoring, voorspelling, prognose, behandeling of verlichting van ziekten.[15] De fabrikant moet wel specifiek dat medisch doel voor ogen hebben. Als een ziekenhuis besluit om spreadsheetsoftware in te zetten voor het bijhouden van bloedwaardes, is die software dus nog géén medisch hulpmiddel. Maar een AI-toepassing die zelf patiënten diagnosticeert of testuitslagen beoordeelt, zal al snel als medisch hulpmiddel kwalificeren.

14. Zie ook overweging 19 bij de MDR.
15. Zie ook artikel 2 lid 1 van de MDR.

Voor medische hulpmiddelen bestaat in Europa al een uitgebreid regelgevend kader. Tot voorkort gold hiervoor de Richtlijn medische hulpmiddelen, welke inmiddels is vervangen door de MDR. De regels uit de MDR zijn hoofdzakelijk bedoeld om de veiligheid van medische hulpmiddelen te borgen en daarmee ook de gezondheid van de Europese burger. Dat is een vergelijkbaar doel als hetgeen wordt nagestreefd met de nu aangekondigde Wet AI.[16] Het gevolg daarvan is dat er op diverse vlakken overlap bestaat tussen de Wet AI en de MDR. De wetgever heeft zijn best gedaan om daar rekening mee te houden, maar toch lijken de Wet AI en de MDR nog niet op alle vlakken even goed op elkaar aan te sluiten. Hieronder lichten wij dit toe aan de hand van drie concrete voorbeelden.[17]

16. Vergelijk overweging 4 bij de MDR en overweging 5 bij de Wet AI.
17. Dit is nadrukkelijk geen uitputtend overzicht van de paralellen tussen de verschillende regelgevingsinstrumenten. Zo bevatten de Wet AI en MDR bijvoorbeeld ook (overlappende) bepalingen over het opzetten van een kwaliteitsbeheersysteem, het bijhouden van technische documentatie en het registreren van de AI-toepassing c.q. het medisch hulpmiddel in een Europese databank.

Risicomanagement

Een van de centrale verplichtingen uit de Wet AI is het inrichten van een systeem voor risicobeheer.[18] Een soortgelijke verplichting bestaat echter óók al onder de MDR.[19] Hoewel de naam iets afwijkt (in de MDR wordt gesproken over een risicomanagementsysteem) is de strekking ervan hetzelfde. Men moet in kaart brengen welke risico's er gepaard gaan met de inzet van het medisch hulpmiddel c.q. de AI-toepassing en moet vastleggen welke maatregelen er genomen zijn om deze risico's te beperken. Het systeem moet periodiek gecontroleerd en zo nodig geactualiseerd worden.

Het is in onze optiek niet erg praktisch om één concreet vraagstuk te regelen in verschillende wetgevingsinstrumenten. Dit maakt het voor marktpartijen erg ingewikkeld om in kaart te brengen aan welke regels zij nu precies moeten voldoen. Voor het inrichten van een risicomanagementsysteem onder de MDR bestaan momenteel al duidelijke kaders.[20] Door nieuwe wetgeving 'naast' de MDR te leggen wordt het geheel erg ondoorzichtig. In hoeverre kan men in de toekomst nog met een MDR-beheersysteem volstaan? Deze vraag wordt door de Europese Commissie vooralsnog niet beantwoord.

18. Zie artikel 9 van de Wet AI.
19. Zie artikel 10 van de MDR.
20. Zie in dit kader ISO 14791:2019.

Interessant is in dit kader ook dat de Wet AI de verantwoordelijkheid voor het risicobeheersysteem primair bij de *aanbieder* neerlegt, terwijl deze onder de MDR bij de *fabrikant* berust.[21] Hoewel deze definities aardig bij elkaar in de buurt komen, zijn deze niet exact hetzelfde. Een aanbieder in de zin van de Wet AI is (kort samengevat) iemand die een AI "ontwikkelt of daarover beschikt". Een fabrikant in de zin van de MDR is degene die een hulpmiddel "vervaardigt of laat vervaardigen". Daarmee lijkt de Wet AI een breder toepassingsbereik te hebben; je hoeft immers alleen maar over de AI te "beschikken". Hier zie je direct hoe het een met het ander kan gaan schuren. Als je een aanbieder bent onder de Wet AI, maar niet de fabrikant onder de MDR – in hoeverre ben je dan straks verantwoordelijk voor de inrichting van een risicomanagementsysteem?[22]

21. Vergelijk artikel 16 sub a jo. artikel 9 van de Wet AI en artikel 10 van de MDR.
22. Dergelijke definitiekwesties spelen ook bij diverse andere verplichtingen uit de Wet AI, zoals de conformiteitsbeoordeling. Vergelijk artikel 16 van de Wet AI en artikel 10 van de MDR.

Conformiteitsbeoordeling

Zowel de MDR als de Wet AI stellen een zogeheten conformiteitsbeoordeling verplicht. Deze conformiteitsbeoordeling moet worden uitgevoerd door een onafhankelijke instantie.[23] Als de beoordeling succesvol is, krijgt men een CE-markering die in/aan/op de AI-toepassing c.q. het medisch hulpmiddel moet worden vermeld. De Europese Commissie benadrukt dat het niet de bedoeling is om een 'dubbele' conformiteitsbeoordeling te laten plaatsvinden. Uit de overwegingen bij de Wet AI blijkt expliciet dat wanneer er al een conformiteitsbeoordeling plaats moet vinden onder de MDR er niet óók nog een beoordeling op grond van de Wet AI vereist is.[24] Op die manier worden dubbele lasten voorkomen.

23. Rekening houdend met het feit dat alleen medische hulpmiddelen uit risicoklasse IIa of hoger als hoog risico toepassing worden aangemerkt onder de Wet AI. Zie ook voetnoot 10.
24. Zie overweging 30 bij de Wet AI.

Maar hoewel er slechts één conformiteitsbeoordeling hoeft te worden uitgevoerd, is het momenteel nog wel de vraag hoe die beoordeling er concreet uit moet komen te zien. Want uit de Wet AI vloeien de nodige verplichtingen voort die als zodanig *niet* in de MDR geregeld zijn. In hoeverre moeten die nieuwe verplichtingen straks worden meegenomen in de conformiteitsbeoordeling? En zijn de 'notified bodies' wel in staat om die nieuwe verplichtingen te controleren? De Europese Commissie geeft hier slechts zeer beperkte informatie over. Zo wordt genoemd dat de Wet AI "geen gevolgen mag hebben voor de methode of algemene structuur van de [bestaande] conformiteitsbeoordeling" onder de MDR.[25] Wat dat precies betekent, wordt nergens uitgelegd.

25. Zie ook overweging 63.

Toezicht op naleving

Afsluitend verdient ook het toezichtkader kort de aandacht. Hoe het toezicht op de Wet AI in de toekomst precies zal worden ingericht, laat zich op dit moment nog moeilijk voorspellen. Wel valt uit de Wet AI al op te maken dat er in iedere lidstaat een toezichthouder zal moeten worden aangewezen.[26] Daarnaast komt er een overkoepelend Europees Comité waarbinnen afstemming en samenwerking plaatsvindt.[27] Als er straks een nieuwe toezichthouder komt voor naleving van AI-wetgeving: hoe verhoudt deze zich dan tot bestaande autoriteiten? We hebben in Nederland immers al de Inspectie Gezondheidszorg en Jeugd (IGJ). Is een AI-aanbieder straks aan twee verschillende autoriteiten verantwoording verschuldigd? En als er overtredingen worden geconstateerd, wie gaat er dan handhaven?

26. Zie artikel 59 van de Wet AI.
27. Zie artikel 56 van de Wet AI.

Ook voordelen?

Hoewel er nog de nodige haken en ogen aan de Wet AI zitten, zien wij een aantal positieve kanten aan de Wet AI. Zo bevat het voorstel diverse aanvullende eisen die de kwaliteit, veiligheid en betrouwbaarheid van (medische) AI-toepassingen verder kunnen verbeteren. Denk aan de eisen op het gebied van kwaliteit aan data[28], maar ook aan de verplichtingen om transparant te zijn over de werking van de AI.[29] De vraag is echter of de nu gekozen aanpak de meest pragmatische oplossing is. Is het niet veel overzichtelijker om in de MDR (en eventuele andere sectorspecifieke wetgevingsinstrumenten) een aantal aanvullende regels op te nemen om specifieke AI-risico's af te hechten? Op die manier hebben we mogelijk wel de baten maar niet de lasten van het voorstel dat nu op tafel ligt.

28. Zie artikel 10 van de Wet AI.
29. Zie artikel 13 van de Wet AI.

Alexander Freund
Information security consultant

Security

Twee eisen aan leveranciers-management

De coronapandemie heeft binnen de zorg voor een versnelling van de digitalisering gezorgd. Zo zijn talloze zorgaanbieders sindsdien gaan beeldbellen met hun patiënten als oplossing voor de vele fysieke beperkingen die werden opgelegd. Vaak was dit beeldbellen geen onderdeel van de dagelijkse praktijk en zijn er soms met enige haast beeldbelapplicaties aangeschaft. Dit is vanwege de haast vermoedelijk vaak gebeurd zonder volledige aandacht voor de informatiebeveiligingsaspecten van de leveranciers. Aangezien de zorgaanbieder zelf verantwoordelijk is voor het leveren van goede (digitale) zorg, moet de zorgaanbieder veel aandacht besteden aan het aspect informatieveiligheid bij het selecteren van een leverancier, onder andere op grond van NEN 7510. In dit artikel wordt ingegaan op de beheersdoelstellingen in het kader van leveranciersrelaties conform NEN 7510 en hoe daaraan voldaan kan worden.

Door het gebruik van (standaard) inkoopvoorwaarden en een verwerkersovereenkomst wordt er al de nodige aandacht besteed aan informatiebeveiliging bij het selecteren van een leverancier. NEN 7510 bevat echter specifieke eisen, die niet altijd geregeld kunnen worden door inkoopvoorwaarden en/of een bepaalde verwerkersovereenkomst op te leggen.

NEN 7510 beschrijft twee beheersdoelstellingen in het kader van leveranciersrelaties:

1. Informatiebeveiliging in leveranciersrelaties
De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers (NEN 7510-2:2017, §15.1).

2. Beheer van dienstverlening van leveranciers

Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met deA leveranciersovereenkomsten handhaven (NEN 7510-2:2017, §15.2).

Informatiebeveiliging

Bij de eerste doelstelling komt het erop neer dat er risico's voor de bescherming van informatie ontstaan, wanneer leveranciers toegang of beschikking krijgen over bedrijfsmiddelen. Vanuit het perspectief van beeldbellen kan hier bijvoorbeeld gedacht worden aan het opslaan van beeldbelgesprekken op de servers van een leverancier. Een eis kan dan zijn dat de leverancier zulke gesprekken niet mag opslaan op haar servers of, indien dat wel gebeurt, alleen de zorgaanbieder er toegang toe heeft en dat de informatie versleuteld wordt opgeslagen.

De drie standaard uitgangspunten om een risicobeoordeling op dit vlak uit te voeren zijn beschikbaarheid, integriteit en vertrouwelijkheid. Voor beeldbellen zal in de meeste gevallen de vertrouwelijkheid van de uitgewisselde informatie het belangrijkst zijn en daarna pas de beschikbaarheid en integriteit. Voor de beschikbaarheid van de dienst kijkt men dan bijvoorbeeld naar het voorhanden zijn van alternatieven of het simpelweg doorschuiven van afspraken. Dit zou anders zijn indien van een medisch expert verwacht wordt dat hij of zij deelneemt via beeldbellen aan een spoedeisende operatie.

Om de eerste doelstelling te behalen zullen er een aantal stappen gezet moeten worden bij de leveranciersselectie.

Stap 1: leg duidelijke regels op aan medewerkers en leveranciers

Stap 1 is om beleid te hanteren met betrekking tot leveranciers. De norm schrijft voor dat de organisatie eisen opstelt en deze met elke leverancier afspreekt. De risico's die samenhangen met de toegang die de leverancier heeft tot bedrijfsmiddelen worden daarmee verkleind. Met andere woorden: zorg er niet alleen voor dat er duidelijke regels zijn voor de eigen medewerkers, maar leg die regels ook op aan leveranciers.

Stap 2: Documenteer de beveiligingseisen per leverancier

Stap 2 schrijft voor dat 'alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt'. Oftewel: bepaal bij elke leverancier die toegang heeft tot informatie of IT welke beveiligingseisen nuttig zijn. Zorg dat de afspraken netjes worden gedocumenteerd in een contract. Dan kan daar later geen misverstand over ontstaan.

Stap 3: houd grip op partijen verderop in de keten

Net zoals leveranciers een risico vormen voor de bedrijfsmiddelen van de organisatie, kunnen onderaannemers van de leverancier ook een risico vormen. Het is daarom belangrijk om óók grip te houden op partijen verderop in de keten. Als derde stap schrijft NEN 7510 daarom voor dat contracten met leveranciers eisen moeten bevatten om de risico's in verband met de toeleveringsketen te beheersen. Hierbij kan onder andere worden gedacht aan een verplichting om eisen die de leverancier op zich neemt ook op te leggen aan andere partijen in de keten.

Beheer van dienstverlening

De tweede doelstelling is erop gericht om een vooraf bepaald niveau van beveiliging en dienstverlening te handhaven, in lijn met de gemaakte afspraken. Deze doelstelling draait dus niet in directe zin om het beschermen van bedrijfsmiddelen van de organisatie, maar meer om het in de gaten houden of de leverancier doet wat hij beloofd heeft.

In het kort komt de tweede doelstelling erop neer dat de dienstverlening van leveranciers regelmatig gemonitord, beoordeeld en geaudit moet worden. Daarnaast moet er regelmatig beoordeeld worden welke veranderingen er zijn geweest in de dienstverlening van leveranciers, welke risico's daaraan kleven en hoe groot die risico's precies zijn. Op deze wijze kan tijdig worden bijgestuurd om die risico's tot een acceptabel niveau te beperken. Voordat men hieraan toekomt, zal er eerst een leverancier geselecteerd moeten worden die voldoet aan de gestelde eisen.

ICTRECHT
security

Uw organisatie goed beschermd met ICTRecht Security

ICTRecht Security werkt samen met u aan een veilige organisatie. Wij helpen u om grip te krijgen én te houden op informatiebeveiliging. Zo zorgt u ervoor dat uw security aantoonbaar op orde is en waarborgt u de continuïteit van uw bedrijfsprocessen.

Altijd beschikken over deskundige security ondersteuning? Kies dan voor ICTRecht Security. Wij zijn direct inzetbaar en altijd beschikbaar (24/7). ICTRecht Security staat voor flexibiliteit: u bepaalt wat wij voor u doen en onze abonnementen zijn per maand opzegbaar.

Meer weten?
Ga naar: ictrecht.nl/security
Of neem contact op via:
020 663 1941

Iris de Groot
Juridisch adviseur

E-health Privacy Innovatie

Het delen van persoonsgegevens via blockchain in de zorg

De zorg is continu bezig met het sneller en soepeler organiseren van de informatievoorzieningen en gebruikte processen. Het doel hiervan is onder meer de burger meer inzicht en regie te geven over informatie. De behoefte om op een veilige wijze rechtstreeks gegevens te delen neemt dus toe. Blockchain is een techniek die wordt genoemd om aan deze behoefte te kunnen voldoen.

Blockchain biedt kansen, maar de toekomstige toepassing werpt ook nog veel vragen op, onder andere op het gebied van privacy. Het delen van gevoelige (persoons)A gegevens is gebonden aan verschillende wet- en regelgeving. De Algemene verordening gegevensbescherming (AVG) maakt hier deel van uit. In dit artikel ga ik in op het gebruik van blockchain in de zorg en het plaatsen van persoonsgegevens op de blockchain.

Mens en techniek

Arbeidskracht is een uitdaging in de zorg. Met name als we kijken naar de toekomst, waarbij de kosten voor het leveren van zorg stijgen.[1] Veel van het werk in de zorg is namelijk niet te automatiseren of te vervangen door een techniek, het blijft voor een groot deel mensenwerk. Ondanks dat zien we wel verschillende technieken in de zorg die het personeel ondersteunen. Blockchain kan deel uitmaken van deze ondersteuning, door te zorgen voor een betrouwbare informatie-uitwisseling tussen apparaten.

1. Zie ook het coalitieakkoord 'Omzien naar elkaar, vooruitkijken naar de toekomst', 15 december 2021.

Kenmerken van blockchain

Door de onderscheidende kenmerken van blockchain is er sprake van een betrouwbare vastlegging van gegevens.[2] Dit heeft te maken met cryptografie en

encryptie. In de zorg is het van groot belang dat derden de informatie niet in handen krijgen. Grote datalekken en incidenten moeten voorkomen worden. Daarnaast is blockchain een gedecentraliseerde en gedistribueerde database. Deze database bevat gegevens die permanent worden opgeslagen en (vrijwel) niet kunnen worden gewijzigd. De gegevens worden namelijk vastgelegd in blokken. De inhoud van elk blok kan verschillen. Het eerste blok kan bijvoorbeeld informatie bevatten over toestemming. Het volgende blok kan vervolgens informatie bevatten over het intrekken van de toestemming en op welke dag en tijd dat heeft plaatsgevonden. Blockchain biedt de mogelijkheid dat elk gegeven, dat wordt toegevoegd aan het blok, automatisch wordt gecontroleerd. Dit maakt het grootschalig verwerken van data mogelijk. Miljoenen gegevens kunnen redelijk eenvoudig worden gecontroleerd op basis van een algoritme.

2. De betrouwbaarheid is wel afhankelijk van de input. De output is niet betrouwbaar bij fouten in de input.

De controle bestaat uit een wiskundige functie die de cryptogratischehashfunctie wordt genoemd. De gegevens worden verwerkt in de blockchain en vervolgens vertaald naar unieke codes (de hashwaardes).[3] Het is praktisch onmogelijk dat de invoer van de verschillende data leidt tot eenzelfde hashwaarde. Daarnaast kan de hashwaarde niet aan verschillende data worden gekoppeld.

3. Encryptie en de hashfunctie zijn automatiseringstechnieken die worden aanbevolen door Europese privacy toezichthouders omdat er sprake is van gepseudonimiseerde verwerking van persoonsgegevens. De kans op identificatie blijft dus wel bestaan. Zie Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216.

De hashfunctie zorgt voor een efficiënte controle door middel van het algoritmisch vergelijken van de hashwaardes. Wanneer de hashwaardes identiek zijn, kan ervan uit worden gegaan dat de documenten of ander ingevoerde data, ook identiek zijn. Door de koppeling van de blokken zal een kwaadwillende die gegevens wil aanpassen niet alleen het eerste blok moeten aanpassen, maar ook die van de blokken verderop in de chain.

Een kwaadwillende die een transactie wil aanpassen zal niet alleen de hashwaarde, en dus ook hash pointer van het desbetreffende blok moeten aanpassen, maar ook die van de blokken verderop in de chain.

Het is een betrouwbare oplossing voor het vastleggen van gegevens. Daarbij zorgt het voor transparantie. Elke toevoeging is namelijk zichtbaar voor het gehele netwerk dat deelneemt aan de blockchain. Een fout of onjuiste toevoeging kan daarom gemakkelijk en snel opgespoord worden.

Kansen voor de zorginfrastructuur

Het gebruik van blockchain is nog abstract. Blockchain staat dus voor betrouwbaarheid en transparantie, maar het is ook een techniek waarover nog veel onduidelijkheid bestaat en de toepassingen (nog) niet uitgekristalliseerd zijn. In de praktijk blijkt dat de blockchain met name gebruikt kan worden voor binaire processen. Dit betekent dat het moet gaan om een duidelijke uitkomst, een ‘ja’ of ‘nee’. Het geven van toestemming kan een binair proces zijn, waarbij het antwoord; (i) ik geef toestemming is of, (ii) ik geef géén toestemming. Het vastleggen van toestemming is dus een voorbeeld van een toepassing voor de blockchain. Daarnaast kan ook gedacht worden aan logging. Hieronder beschrijf ik kort de kansen op dit gebied en de juridische basis.

Toepassing en mogelijkheden blockchain

Van belang bij het geven van toestemming is dat deze vrij, geïnformeerd, ondubbelzinnig en specifiek gegeven moet worden.[4] Het moet voor de betrokkene dus heel duidelijk zijn waarvoor de toestemming moet worden gegeven – dus welk doel de toestemming dient. Toestemming kan ook op elk moment weer ingetrokken worden en er dient sprake te zijn van een duidelijke actieve handeling.

4. Artikel 6, lid 1, onder a, AVG.

Met name het intrekken van toestemming is soms problematisch. Dit moet namelijk op een vergelijkbare wijze kunnen plaatsvinden als het geven van toestemming. Er mogen geen drempels worden opgelegd voor het geven van toestemming en het vervolgens intrekken. Bij het geven of intrekken van toestemming dient altijd een registratie plaats te vinden.

Blockchain kan ervoor zorgen dat de toestemming wordt opgeslagen en op elk moment weer kan worden ingetrokken. Als de betrokkene de toestemming heeft gegeven via een app of website, dan is het intrekken van de toestemming door middel van blockchain op dezelfde wijze mogelijk.

Blockchain kan dus een basis bieden voor de bouwstenen van de infrastructuur in de zorg. Het vast-

leggen van toestemming is hiervan een voorbeeld. Een ander proces waarbij het gebruik van de blockchain interessant is, is logging.

Het vereiste om te loggen zien we in verschillende wet- en regelgeving terug, waaronder in de AVG. De AVG biedt een algemeen recht op inzage (artikel 15 AVG).[5] De Wet op de geneeskundige behandelingsovereenkomst (WGBO) bevat aanvullingen op dit algemene inzagerecht van de AVG. Ook op grond van de WGBO heeft de betrokkene recht op inzage in- en afschrift van het medische dossier (artikel 7:456 Burgerlijk Wetboek). Daarnaast is sinds vorig jaar (1 juli 2020) de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) van kracht. Op basis van deze wetgeving heeft de betrokkene recht op inzage en/of afschrift. In het afschrift dient op verzoek loggingsinformatie te worden opgenomen.[6]

5. Artikel 15 AVG geeft daarnaast ook aan dat er informatie aan de betrokkene moet worden verstrekt over de herkomst van de gegevens.
6. Zie onder andere artikel 15e Wabvpz. Dit artikel is van toepassing bij het gebruik van een elektronisch uitwisselingssysteem. Dit vereiste is ook terug te lezen in het Besluit elektronische gegevensverwerking in de zorg. Daarnaast volgt logging impliciet uit artikel 32 AVG.

Voor de zorg is het gebruikelijk om de NEN-normen als uitgangspunt te nemen voor het inregelen van de juiste beheers- en beveiligingsmaatregelen. De NEN 7513 ziet specifiek op logging in de zorg. Duidelijk moet dus zijn wie wanneer welke informatie heeft geraadpleegd. Om te achterhalen wie toegang heeft gehad tot de gegevens kan eveneens worden gedacht aan het gebruik van blockchain.

Blockchain is dus interessant vanwege de onderscheidende kenmerken. Het integreren van bovenstaande processen in de blockchain behoort tot de mogelijkheden en kan verschillende voordelen opleveren. Eén van deze voordelen is de transparantie. De gegevens kunnen moeilijk worden gewijzigd. Dit wordt ook wel "single source of truth" genoemd.

Single source of truth

Het moeilijk wijzigen van gegevens klinkt ten aanzien van beveiligingsaspecten aantrekkelijk. Echter, dit kan ook voor problemen zorgen. Persoonsgegevens die in de blokken worden opgeslagen kunnen in de toekomst dus ook moeizaam of niet weer worden verwijderd.[7] Ook een wijziging van de gegevens is een verwerking in een nieuw blok en maakt de eerdere verwerking niet ongedaan. Als er dus persoonsgegevens worden opgeslagen in de zorg in een blockchain, dan is de kans aanzienlijk dat het hierbij gaat om bijzondere persoonsgegevens.[8] De verwerking van deze persoonsgegevens kan niet oneindig zijn. Er dient vastgelegd te worden wat de bewaartermijn van de persoonsgegevens is en welk doel de verwerking dient.[9]

7. Verwijdering is een recht van de betrokkene. Zie voor de rechten van betrokkenen artikel 12-23 AVG.
8. Er geldt een verbod op de verwerking van bijzondere persoonsgegevens. De algemene doorbrekingsgronden staan beschreven in artikel 9 AVG en de artikelen 22 tot en met 33 van de Uitvoeringswet AVG (UAVG).
9. Artikel 5-11 AVG.

Het is technisch een uitdaging om invulling te geven aan de verplichting om persoonsgegevens te verwijderen. Een algemene blockchain gebruiken om de gegevens van betrokkenen op vast te leggen is dus op dit moment niet mogelijk. De unieke kenmerken maken de verwijdering namelijk vrijwel onmogelijk.

Om tegemoet te kunnen komen aan de verwijdering en/of de passelijke bewaartermijn kan wel een persoonlijke blockchain gehanteerd worden. Bij een persoonlijke blockchain worden de gegevens van één betrokkene verwerkt door een beperkt aantal deelnemers (bijvoorbeeld de gegevens van een patiënt die worden verwerkt door zorgmedewerkers). Bij een verzoek of verplichting tot verwijdering kan de blockchain in zijn geheel worden vernietigd.

Echter, op dit moment is bovenstaande nog niet een oplossing die we in de praktijk veel tegenkomen. Vandaar dat de toepassingen waarmee wordt geëxperimenteerd vaak geen persoonsgegevens bevatten. Het gaat dus om die binaire processen, die goed te verwerken zijn in de blockchain. De daadwerkelijke persoonsgegevens worden dan off-chain opgeslagen. Door het gebruik van pointers naar de off-chain opgeslagen persoonsgegevens kan de link worden gelegd naar de juiste persoonsgegevens, maar is verwijdering ook mogelijk.

Verwijdering moet in dit kader meer worden gezien als het ontoegankelijk maken van de betreffende link/de pointer. Want ook hierbij kan de pointer niet worden verwijderd uit de blockchain. Er mogen bij het creëren van de pointer dus geen persoonsgegevens worden gebruikt. Het niet kunnen raadplegen van de

pointer zorgt er enkel voor dat de persoonsgegevens niet meer raadpleegbaar zijn. Aangezien de pointer dan geen persoonsgegevens bevat, is het geen probleem dat deze blijft staan in de blockchain.

Het voordeel aan bovenstaande is dat de pointers ook tijdelijk ontoegankelijk kunnen worden gemaakt. Mocht een betrokkene bezwaar hebben gemaakt tegen een verwerking of is er om een andere reden vereist dat de verwerking wordt beperkt, dan kan de link tijdelijk worden doorgeknipt.

Blockchain kan een goede aanvulling zijn

De uitdagingen in de zorg nemen naar verwachting de aankomende jaren toe. De kosten lopen op en er zijn meer en meer medewerkers nodig om de juiste zorg te kunnen bieden. Daarbij neemt de complexiteit aan technieken toe en het samenspel hiervan is soms moeilijk te duiden. Het gebruik van blockchain kan een goede aanvulling zijn wanneer het gaat om het vastleggen van gegevens en het koppelen van processen.

Door de encryptie- en hashingtechniek van de blockchain is het gebruik van de blockchain interessant wanneer het gaat om gegevens die geen persoonsgegevens zijn. Het zorgt voor transparantie en een betrouwbare vastlegging. Bij het geven van toestemming of logging worden enkel de bevindingen vastgelegd. Dit kan mogelijkheden geven voor het organiseren van de processen en het automatisch inregelen van de registratie.

De verwerking van persoonsgegevens op de blockchain heeft dus niet de voorkeur. De gegevens kunnen (vrijwel) onmogelijk nog verwijderd worden – als het gaat om een algemene blokchain. Een alternatief is een persoonlijke blockchain, waar enkel de gegevens van één persoon op worden vastgelegd. De volledige blockchain dient dan te worden vernietigd bij een verzoek tot verwijdering of bij het eindigen van de bewaartermijn.

Itte Overing
Juridisch adviseur

E-health Security

Zorgaanbieder, kan uw patiënt al veilig inloggen?

Toegang tot zorgapplicaties moet straks voldoen aan de Wet digitale overheid (Wdo).[1] De eerste tranche van de Wdo regelt het veilig en betrouwbaar inloggen door Nederlandse burgers en bedrijven bij de (semi-)overheid. Zorg valt onder de semi-overheid.

Wdo, eerste tranche

De Wdo is nu nog een wetsvoorstel. Het is de bedoeling dat de (semi-)overheid veilig en overzichtelijk digitaal kan gaan samenwerken met de burger en het bedrijfsleven. De wet is opgesteld als kaderwet met algemene principes zodat er mee bewogen kan worden met ontwikkelingen en wensen. In lagere wetgeving worden de algemene principes uitgewerkt.

De Wdo zal gaan gelden voor niet alleen de overheid en de rechterlijke macht, maar ook voor aangewezen organisaties zoals zorgorganisaties. De eerste tranche van de Wdo regelt dat zorgorganisaties:

- hun diensten moeten indelen op de volgende betrouwbaarheidsniveaus: Laag, Substantieel of Hoog. Dit zijn de drie betrouwbaarheidsniveaus zoals gehanteerd in de eIDAS-verordening;[2]
- toegang moeten verlenen middels eID en hebben zij een acceptatieplicht voor inlogmiddelen die voldoen. Het gaat dan om DigD (althans de verbeterde versie) maar ook om private inlogmiddelen. Het ETSI, Europees Telecommunicatie en Standaardisatie Instituut, heeft goede standaarden opgezet voor deze inlogmiddelen;
- moeten meebetalen voor de inlogmiddelen zoals gebruikt door patiënten/cliënten; en
- hun informatiebeveiliging op orde moeten hebben.

Op digitaleoverheid.nl wordt ook al ingegaan wat in het verschiet ligt, wat de tweede tranche zal brengen. Denk hierbij aan onderwerpen zoals het verantwoord delen van digitale persoonsgegevens binnen en buiten de overheid; het beleggen van de verantwoordelijkheid voor het stelsel van basisregistraties; en hoe kunnen het burger- en bedrijvendomein in de Wdo verder naar elkaar toegroeien. Omdat nog niet duidelijk is wat zal gaan gelden voor zorgorganisaties, wordt hier niet verder op ingegaan.

“De Wdo eist dat zorgaanbieders een veilige en betrouwbare manier van inloggen bieden aan hun patiënten wanneer zij hen digitaal toegang verlenen tot hun medische gegevens.”

Itte Overing
Juridisch adviseur

Zorgaanbieder of ICT-leverancier

De Wdo eist dat zorgaanbieders een veilige en betrouwbare manier van inloggen bieden aan hun patiënten wanneer zij hen digitaal toegang verlenen tot hun medische gegevens. Praktisch gezien zal de ICT-leverancier deze inlogmiddelen moeten implementeren in het patiëntportaal of de persoonlijke gezondheidsomgeving indien geboden door de zorgaanbieder.

Het inlogmiddel wordt eID genoemd.[3] Dat refereert aan het feit dat het inlogmiddel zeker moet stellen dat alleen die ene patiënt toegang krijgt tot zijn eigen informatie, er is dus identificatie nodig. Bij eID wordt altijd DigiD genoemd, althans een verbeterde versie van het DigiD. Toch is het zeker de bedoeling dat er ook inlogmiddelen door de private sector worden ontwikkeld en aangeboden, en niet alleen in Nederland maar mogelijk ook vanuit de rest van Europa.

1. https://bit.ly/3ES5xA0.
2. https://bit.ly/3EWxiHM.
3. https://bit.ly/32NnLWn.

Een leverancier van een patiëntportaal zal niet in alle gevallen staan te springen om (ook) een dergelijk inlogmiddel te ontwikkelen en te onderhouden. Bij het onderhoud zal ook doorontwikkeling horen om de beveiliging op het niveau “Substantieel” of “Hoog” te kunnen handhaven. Gevolg is dat het maken van een inlogmiddel dat voldoet aan de regelgeving en de juiste certificeringen heeft, een aparte tak van sport wordt. Daar is een oplossing voor bedacht.

ToegangVerleningService

Dat is de ToegangVerleningService (TVS). Het Ministerie van Volksgezondheid, Welzijn en Sport, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Logius en DICTU hebben samen de TVS ontwikkeld. Middels een koppeling met de TVS kan er in één keer gekoppeld worden met de verschillende eID’s waaronder ook het DigiD. Het idee is dat elke patiënt (en burger) dan vrij kan kiezen welk eID hij gebruikt. Via de koppeling met de TVS kan er dan ingelogd worden bij de dienst van de specifieke ICT-leverancier. De ICT-leverancier hoeft dan dus niet allerlei koppelingen met verschillende eID-leveranciers te onderhouden.

Er is door de overheid een factsheet opgesteld over het koppelen met TVS. Zowel voor de zorgaanbieder als voor de ICT-leverancier is informatie opgenomen over welke stappen ondernomen moeten worden om te koppelen met de TVS en zo te gaan voldoen aan de Wdo.

Beveiligingsniveau inlogmiddel

Een patiënt/cliënt moet over een inlogmiddel kunnen beschikken waarmee hij of zij veilig en betrouwbaar kan inloggen op een applicatie waarmee hij of zij inzicht krijgt in zijn of haar medische gegevens. Op dit moment biedt de overheid ons het DigiD. Daarover zegt de overheid nu zelf:

“(…)Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD.”

Het is de bedoeling dat DigiD in eerste instantie het beveiligingsniveau Substantieel gaat bieden en uiteindelijk ook Hoog. Als voorbeeld, voor toegang tot medische persoonsgegevens zal tenminste het niveau Substantieel nodig zijn. Het uiteindelijk vereiste niveau voor toegang tot het EPD zal Hoog zijn, omdat het hier gaat om medische persoonsgegevens die vallen onder het beroepsgeheim.[4]

Maar wat houdt Hoog dan in, in de praktijk? Voor de patiënt zal zichtbaar zijn dat er meer eisen worden gesteld aan de identificatie, het middel zal alleen uitgegeven worden als de patiënt zich op een bepaalde manier heeft geïdentificeerd. Minder zichtbaar zal zijn dat er ook hogere eisen worden gesteld aan bijvoorbeeld de versleuteling van data.

Informatiebeveiliging

Met het op orde hebben van informatiebeveiliging wordt bedoeld dat de zorgorganisatie beschikbaarheid, integriteit en vertrouwelijkheid borgen, en tevens aandacht hebben voor authenticiteit, onweerlegbaarheid, transparantie en flexibiliteit. In de Memorie van Toelichting bij de Wdo wordt aangegeven dat dit gerealiseerd zal worden middels nadere regels (Algemene Maatregel van Bestuur). Hierbij wordt gekeken naar de geldende rijksbrede informatieveiligheidsnormen. Oftewel: voorzichtige inschatting is dat voor zorgorganisaties NEN 7510 naar voren gaat worden geschoven. Waarbij dan wellicht ook concrete invulling van de beveiligingsmaatregelen wordt voorgeschreven, afgestemd op het passende betrouwbaarheidsniveau. Maar dat is dus wel nog even speculatie.

Wijziging

1 juli 2021 zou de Wdo worden ingevoerd. De invoering is uitgesteld tot in ieder geval medio 2022.[5] De redenen zijn dat eerst een aanpassing in het kader van de bescherming van persoonsgegevens in relatie tot de positie van (grote) private technologie ondernemingen moest worden geformuleerd, en dat deze aanpassing moet worden voorgelegd aan de Kamer. De aanpassing is in de vorm van een novelle aangeboden.[6] Staatsecretaris van Binnenlandse Zaken en Koninkrijkrelaties (drs. R.W. Knops) schrijft in zijn Memorie van Antwoord hierover:

"Teneinde nog beter tegemoet te komen aan de geuite vragen en zorgen, ben ik voornemens een wetswijziging in te dienen waarbij het verhandelverbod inzake gegevens, privacy by design en open source als hoofdelementen van de te regelen materie wettelijk worden verankerd."[7]

Oftewel:

- Een verhandelverbod voor gegevens: het verdienmodel van de private partij moet ook gericht zijn op het identificatiemiddel (en dus niet op het exploiteren van persoonsgegevens). Daarom zal ook getoetst worden of er een directe relatie is tussen de vergoeding en de geleverde dienst (inlogmiddel), of dat het vanuit elders in de eigen organisatie wordt gefinancierd.[8] Verder is profilering niet toegestaan. Loggegevens mogen niet aan personen kunnen worden gekoppeld, behalve voor zover nodig om incidenten en misbruik op te sporen. Daartoe wordt een plicht opgenomen om gebruiks- en gebruikersgegevens gescheiden op te slaan.[9]
- Privacy by design: partijen zijn direct op grond van de Algemene verordening gegevensbescherming verplicht om privacy by design toe te passen, en de Autoriteit Persoonsgegevens houdt toezicht. In de aanpassing van het voorstel wordt nu ook verankerd dat dit een afwijzingsgrond is voor een erkenningsaanvraag, voor zover het principe niet voldoende wordt toegepast. Om te voorkomen dat het een momentopname is, en er later niet meer wordt voldaan aan de stand der techniek, kan de erkenning ingetrokken, opgeschort of gewijzigd worden.
- De verankering van open source: er moet voldoende gebruik worden gemaakt van open source software. Het uitgangspunt hierbij is: open source, tenzij… Wel wordt hierbij een groeimodel gehanteerd: al is het nu logisch om closed source te accepteren om bijvoorbeeld veiligheids- en continuïteitsproblemen te voorkomen, dat hoeft over een paar jaar niet meer zo te zijn omdat er dan wel open source software voor handen is met een sterke community die het (door-) ontwikkelt en onderhoudt.

U heeft nog even

De vroegst mogelijke datum van inwerkingtreding is 1 juli 2022. Of het 1 juli wordt of later, hangt af van wanneer de Kamer het voorstel met de wijziging in het kader van de privacybescherming bespreekt. Wilt u alvast aan de slag met de Wdo? Bekijk dan in ieder geval even de factsheet over de TVS.

4. https://bit.ly/3HwxXRZ.
5. https://bit.ly/3znRh0K.
6. https://bit.ly/3FUDgdE.
7. P 12, MvA bij wetsvoorstel digitale overheid.
8. P. 12, MvA bij wetsvoorstel digitale overheid.
9. P. 14, MvT bij wijziging v.h. wetsvoorstel digitale overheid.

Sari Jansen
Juridisch adviseur

E-health Contracteren

De online behandeling (sovereenkomst)

U bent tegenwoordig slechts één muisklik verwijderd van een online platform waar een specialist u eenvoudig en snel kan voorzien van een antwoord op uw medische hulpvraag. De laagdrempeligheid van het op afstand en online verlenen van zorg heeft echter niet tot het ogenschijnlijk logische gevolg dat bepaalde verplichtingen niet of verminderd gelden. In dit artikel beantwoorden we de vraag of er bij het bieden van online (medische) hulp een behandelingsovereenkomst tot stand komt en zo ja, aan welke (wettelijke) verplichtingen de hulpverlener en diens ICT-leverancier vervolgens moeten voldoen.

De behandelingsovereenkomst

De Wet op de geneeskundige behandelingsovereenkomst (WGBO) regelt allerlei randvoorwaarden voor de samenwerking tussen de patiënt en een medisch specialist, in deze wet als 'hulpverlener' aangeduid. De hulpverlener moet bijvoorbeeld op grond van deze wet een medisch dossier inrichten en heeft een informatieplicht jegens zijn patiënt. Daarnaast heeft hij een medisch beroepsgeheim. De wet is (in ieder geval) van toepassing zodra er sprake is van een behandelingsovereenkomst. Dit is een overeenkomst "waarbij een hulpverlener zich, in de uitoefening van een geneeskundig beroep of bedrijf, tegenover een ander verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, die rechtstreeks betrekking hebben op die ander".[1] De relevante onderdelen uit deze definitie worden hieronder nader toegelicht.

1. Artikel 7:446 lid 1 van het Burgerlijk Wetboek.

Hulpverlener

De hulpverlener is degene die een geneeskundig beroep of bedrijf uitoefent. Aanwijzingen voor de kwalificatie als hulpverlener zijn bijvoorbeeld het min of meer regelmatig verrichten van geneeskundige handelingen en het zich naar buiten kenbaar maken als ge-

neeskundige beroepsbeoefenaar. Denk hierbij aan een psychotherapeut, een tandarts of een verpleegkundige. Ook een rechtspersoon, zoals een ziekenhuis, kan een hulpverlener zijn.

Handeling op gebied van geneeskunst

De hulpverlener moet zich verbinden tot het verrichten van een geneeskundige handeling. Dit is een breed begrip. Een geneeskundige handeling kan bijvoorbeeld het stellen van een diagnose, genezen, preventie en verplegen zijn. Ook het antwoord geven op een concrete medische (hulp)vraag is aan te merken als een dergelijke handeling. Onder een geneeskundige handeling wordt namelijk ook het beoordelen en het geven van raad over de gezondheidssituatie verstaan.

Rechtstreeks betrekking

Om te voldoen aan de kwalificatie van een behandelingsovereenkomst, moet er naast een 'hulpverlener' en een 'handeling op het gebied van geneeskunst' ook sprake zijn van individuele gerichtheid. Dit betekent dat de behandelovereenkomst 'rechtstreeks betrekking moet hebben op de persoon'. Rechtstreeks contact tussen hulpverlener en patiënt is hierbij niet nodig.[2] Als de hulpverlener (een medisch specialist) ingaat op een concrete hulpvraag van een specifieke gebruiker van een online platform, dan is er sprake van individuele gerichtheid. Er kunnen dus via een online platform behandelingsovereenkomsten tot stand komen. Dat betekent dat de hulpverlener (en ICT-leverancier) aan bepaalde wettelijke plichten moet voldoen.

2. KNMG-richtlijn, Niet-aangaan of beëindiging van de geneeskundige behandelingsovereenkomst, KNMG januari 2021, p.7.

Informatieplichten dienst van de informatiemaatschappij

Het aanbieden van online medische hulp via een platform is een vorm van online dienstverlening. Dit betekent dat de dienst gekwalificeerd wordt als een dienst van de informatiemaatschappij. Een leverancier van deze diensten, dat kan ook een hulpverlener of zorgaanbieder zijn, is dan verplicht om bepaalde informatie te verstrekken, zoals het KvK-nummer, vestigingsadres, telefoonnummer en btw-nummer. Alle informatie moet op een gemakkelijk vindbare plaats vermeld worden. Daarnaast gelden er aanvullende informatieverplichtingen als er online ook producten of diensten worden verkocht aan consumenten. Daarop geldt een uitzondering als er bepaalde gezondheidsdiensten worden verleend.[3] Hiervan is sprake als een zorgaanbieder in het kader van de geneeskundige behandelingsovereenkomst medische handelingen op afstand verricht. De ICT-leverancier zal doorgaans niet onder deze uitzondering vallen, maar de hulpverlener of zorgaanbieder wel. In plaats van de aanvullende informatieplichten die op grond van het consumentenrecht gelden, geldt het regime uit de WGBO.

3. Artikel 6:230h lid 2 onder d van het Burgerlijk Wetboek.

Verplichtingen op grond van de WGBO

De behandelingsovereenkomst komt uitsluitend tot stand tussen de gebruiker van een platform en de hulpverlener: het platform zelf is geen partij bij deze overeenkomst. Dat betekent dat de plichten die voortvloeien uit de WGBO gelden voor de hulpverlener en niet voor (de leverancier van) het platform. De leverancier zal wel moeten faciliteren dat de hulpverlener aan haar verplichtingen uit de WGBO kan voldoen. Denk aan verplichtingen als het bieden van adequate hulp en zorg (de zorgplicht, art. 7:453 BW), het informeren van de patiënt op een heldere en adequate wijze (informatie- en overlegplicht, art. 7:448 BW), het bijhouden van een dossier (dossierplicht, art. 7:454 lid 1 en 2 BW), het bewaren van het dossier (bewaarplicht, art. 7:454 lid 3 BW) en het respecteren van de overige patiëntenrechten. Hieruit vloeit onder andere voort dat informatie die via online contact is verkregen van een patiënt in beginsel ook in diens dossier moet worden opgenomen.[4] Dit houdt overigens niet in dat de volledige online gesprekken opgeslagen moeten worden, wel moet de relevante informatie (ook) in het dossier van de patiënt opgenomen worden.

4. KNMG-richtlijn, Omgaan met medische gegevens, KNMG 2020, p.28.

Per januari 2020 is de WGBO gewijzigd. De belangrijkste wijzigingen zijn de aanpassing van de bewaar- en aanvangstermijn van het medisch dossier (20 jaar vanaf de laatste wijziging in het dossier); de aanvulling van de informatieplicht van de hulpverlener en het inzagerecht van nabestaanden. Dit geldt ook wanneer de behandelingsovereenkomst via een platform tot stand is gekomen.

Voor het verlenen van online zorg (op afstand) geldt dat indien er nog geen behandelingsrelatie bestaat het eerste consult tussen hulpverlener en patiënt face-to-face plaats dient te vinden. Om de kans op verspreiding van het coronavirus te verkleinen en de druk op zorgaanbieders te verlichten, heeft de Nederlandse Zorg-

autoriteit (NZa) op deze regel tijdelijk een uitzondering gemaakt. Hulpverleners kunnen het eerste consult met een patiënt nu ook digitaal of telefonisch doen.[5] Afgelopen jaar heeft de versoepeling die is doorgevoerd tijdens de coronacrisis, een definitieve plek in de regels gekregen.[6]

5. https://bit.ly/3EWhDYW.
6. https://bit.ly/3EN1rJH en https://bit.ly/3mQEsXS.

Gedragsregels

Naast de verplichtingen die voortvloeien uit de WGBO, bestaan er in het kader van de gezondheidszorg verscheidene richtlijnen, protocollen en gedragsregels. Een voorbeeld hiervan is de KNMG-richtlijn 'Omgaan met medische gegevens.[7] Een dergelijke richtlijn heeft van zichzelf geen bindende kracht, wel is zij behulpzaam bij het interpreteren van wettelijke bepalingen (bijvoorbeeld het recht van de patiënt op informatie of zorg van een goed hulpverlener). Zo wordt in de eerder genoemde KNMG-richtlijn omschreven wanneer een online consult -waarbij de hulpverlener aan de patiënt een individueel medisch advies geeft- is geoorloofd.[8] Dit is ingevolge de richtlijn alleen geoorloofd als er aan een aantal cumulatieve voorwaarden is voldaan, zoals de voorwaarde dat de identiteit van de patiënt voldoende is vastgesteld en de hulpverlener de patiënt voldoende heeft geïnformeerd over de werkwijze bij online contact.

7. https://bit.ly/3zob9kp.
8. https://bit.ly/3fdBCI4.

Dit jaar zijn er een aantal nieuwe stukken uitgebracht. Zo heeft de KNMG afgelopen januari de vernieuwde richtlijn 'Niet-aangaan of beëindiging van de geneeskundige behandelingsovereenkomst' gepubliceerd, waarin duiding wordt gegeven wanneer de behandelingsovereenkomst kan worden beëindigd.[9] Op grond van de WGBO kan dat immers alleen eenzijdig door de hulpverlener als daar 'gewichtige redenen' voor zijn. In de richtlijn wordt een leidraad gegeven welke ook van toepassing is op behandelingsovereenkomsten die online tot stand zijn gekomen. De richtlijn gaat onder andere in op hoe een behandelingsovereenkomst tot stand komt; welke 'gewichtige redenen' bij eenzijdige opzegging van toepassing kunnen zijn en welke zorgvuldigheidseisen daarbij gelden.

9. https://bit.ly/3qcodGT.

Verder heeft de Patiëntenfederatie Nederland in samenwerking met KNMG, op verzoek van het ministerie van Volksgezondheid, Welzijn en Sport, handen en voeten gegeven aan het inzagerecht in het medisch dossier voor nabestaanden. De Patiëntenfederatie Nederland en KNMG hebben daartoe afgelopen januari een handreiking uitgebracht. Er is een uitgave voor hulpverleners en een uitgave voor patiënten en nabestaanden, met bijbehorende stroomschema's.[10]

10. https://bit.ly/3qpyJuu.

Verplichtingen onder de AVG

Naast verplichtingen die gelden op grond van de WGBO en de gedragsregels die zijn neergelegd in richtlijnen voor de gezondheidszorg, dienen de hulpverlener en ICT-leverancier zich uiteraard ook te houden aan de privacywetgeving: de Algemene verordening gegevensbescherming (AVG). Zo is adequate beveiliging van de verwerkte gegevens noodzakelijk. Voor zorgaanbieders geldt dat zij met medische gegevens werken, welke worden aangemerkt als bijzondere persoonsgegevens. Dit brengt een zwaarder regime met zich mee. Ook voor het verwerken van bepaalde gegevens, zoals het Burgerservicenummer en het BIG-nummer, bestaat een apart regime. Niet alleen de leveranciers van de dienst moeten de zwaardere technische en organisatorische maatregelen in acht nemen, ook de zorgaanbieder zelf moet zich bewust zijn van zijn rol en verantwoordelijkheden.

Denk hierbij in ieder geval aan het gebruik van tweefactor-authenticatie bij de toegang tot het platform en daarnaast aan het bij het gebruik van het platform voldoen aan NEN 7510, NEN 7513 en indien relevant: NEN 7512. Verder kunt u denken aan het uitvoeren van een Data Protection Impact Assessment, indien verplicht, en het sluiten van de benodigde verwerkersovereenkomsten. Voorts moet er gebruik gemaakt worden van privacy-by-design en privacy-by-default. Richting de gebruikers van het platform zal een privacyverklaring gehanteerd moeten worden, waarin onder andere duidelijk is omschreven wat er met hun persoonsgegevens gebeurt.

Voor zowel hulpverleners als ICT-leveranciers is het dus van groot belang kritisch te kijken naar de diensten die feitelijk middels een online platform worden geleverd. Afhankelijk hiervan zullen partijen aan bepaalde verplichtingen moeten voldoen, in het bijzonder wanneer er een behandelingsovereenkomst tot stand komt.

ZORG INNOVATIE FORUM

E-health Innovatie

E-health implementatie in Noord-Nederland

Van onze partner Zorg Innovatie Forum (ZIF)

E-health en zorgtechnologie zijn thema's waarop het Zorg Innovatie Forum[1] (ZIF) actief is. Het ZIF is een netwerkorganisatie in Noord-Nederland en heeft als doel samen te innoveren en inclusie te bevorderen, door middel van ontmoeting, kennisdeling en samenwerking. Het ZIF wil hiermee de kwaliteit van zorg in brede zin in Noord-Nederland structureel verbeteren.

1. www.zorginnovatieforum.nl.

Met de Kenniswerkplaats E-health Implementatie[2] en het project E-health Adaptatie worden verbindingen gemaakt tussen eindgebruikers, ontwikkelaars en zorgprofessionals. De Kenniswerkplaats, die het ZIF samen met de Universiteit Twente en het UMCG begeleidt, dient als plek om kennis en ervaringen te delen en organisaties aan elkaar te matchen. De Kenniswerkplaats E-health Implementatie organiseert vier keer per jaar een online bijeenkomst, die voor iedereen toegankelijk is. Daarnaast ontmoeten leden elkaar op www.werkplaatsimplementatie.com en in een LinkedIn-groep.

2. https://www.zorginnovatieforum.nl/project?id=3.

Eén van de vragen die in het afgelopen jaar voorbij is gekomen, is: wat houdt de implementatie van e-health in de zorg precies in, en welke wet- en regelgeving zijn hierbij van toepassing? In dit artikel gaan wij kort in op deze vraag.

Implementatie van e-health is een vak apart

E-health is een veelomvattend thema. Het gaat namelijk over alle digitale toepassingen in de zorg. Denk aan videobellen met de zorgverlener of het online doorgeven van bloedwaarden. Het heeft betrekking op alles dat u ziet rond informatie- en communicatietechnologie ter ondersteuning of verbetering van de gezondheid en de gezondheidszorg.

Het is een goede ontwikkeling die ook in tijden van vermindert persoonlijk contact uitkomst kan bieden. Vanwege het coronavirus is persoonlijk contact bijvoorbeeld niet altijd mogelijk. Videobellen is een e-health oplossing die in deze gevallen gebruikt kan worden om iemand toch te kunnen spreken. Het implementeren van dergelijke oplossingen is alleen niet eenvoudig. We zien dat er technisch veel kan en wordt ontwikkeld, maar dat implementatie een hobbel is. Daarom is het belangrijk om de eindgebruiker, dus de cliënt of patiënt en de hulpverlener, mee te nemen in het proces van ontwikkeling. Zo wordt de e-health toepassing goed aangesloten bij de wensen van de gebruiker: wat ons betreft een grote voorwaarde!

Selecteren van de juiste leverancier

Er gaat aan heel proces vooraf aan de implementatie van e-health toepassingen. Dit heeft onder andere te maken met de wet- en regelgeving.

Het begint met het selecteren van de juiste leverancier. Vooraf moet duidelijk zijn aan welke eisen deze leverancier moet voldoen. Bij het stellen van deze eisen moet in ieder geval gedacht worden aan beveiligingseisen en welke garanties de leverancier moet bieden. Ook moet gekeken worden naar de verwerking van de persoonsgegevens. Worden de persoonsgegevens bijvoorbeeld doorgegeven aan andere partijen en bevinden deze partijen zich in het buitenland? Dan dient dat meegenomen te worden bij de risicobeoordeling van de oplossing en uiteindelijk bij de selectie van de leverancier.

Privacy van de gebruiker

Naast de selectie van de juiste leverancier is het ook zaak om duidelijk te communiceren met de patiënt of cliënt waar de oplossing voor gebruikt gaat worden. Wat is het doel en hoe gaan de partijen om met de gegevens? Dit kan in een privacy- (en cookie)verklaring en gebruiksvoorwaarden. Begrijpelijkheid is hierbij heel belangrijk. Een patiënt of cliënt wil natuurlijk weten (en begrijpen) wat er met diens gegevens gebeurt.

Behandelingsovereenkomst en zorgplicht

Los van de communicatie en transparantie richting de patiënt of cliënt, moet er ook rekening gehouden worden met de behandeling van de patiënt of cliënt. Of in juridische termen: er is sprake van een behandelingsovereenkomst en een zorgplicht van de hulpverlener. Belangrijk is dat de hulpverlener toestemming vraagt van de patiënt of cliënt. Ook moet voldaan kunnen worden aan rechten als inzage en/of afschrift van de gegevens, opzegging van de behandelingsovereenkomst en aan geheimhouding, bewaartermijn en dossierplicht.

Samen innoveren in de zorg

Voordat u een nieuwe oplossing, zoals videobellen, kunt implementeren, moet dus het één en ander worden gedaan. Betrek de gebruiker tijdig bij de ontwikkeling van de nieuwe toepassing, dat komt de implementatie ten goede. Soms denken patiënten of cliënten dat bijvoorbeeld videobellen een dagelijkse gang van zaken is en binnen een aantal dagen in gebruik genomen kan worden. In de praktijk blijkt er aardig wat tijd overheen te gaan voordat een dergelijke toepassing geïmplementeerd is. De grootste reden is de aandacht voor de rechten van de patiënt of cliënt. Het gaat vaak om gevoelige gegevens waar men zorgvuldig mee dient om te gaan.

Het delen van ervaringen en kennis kan de implementatie versnellen. Elk jaar komen er namelijk meer e-health toepassingen bij. Elke toepassing is weer anders en vraagt om een andere aanpak. Door samen te werken kunnen partijen elkaar helpen bij het innoveren van de zorg. Dat is wat er gebeurd in de Kenniswerkplaats E-health Implementatie en het Noordelijk Platform Zorgtechnologie![3]

3. https://werkgevers.zorgpleinnoord.nl/netwerken/expertmeeting-zorgtechnologie.

Meer weten over de Kenniswerkplaats of over het Zorg Innovatie Forum?
Kijk op www.zorginnovatieforum.nl, stuur een e-mail naar info@zorginnovatieforum.nl of bel naar 050 800 3245.

Itte Overing
Juridisch adviseur

Sanne Haumersen
Juridisch adviseur

E-health Innovatie

ZORG dat u bij bent in 2022

Veel zorgaanbieders zijn hard onderweg om zelfs hun primaire proces, het leveren van zorg, digitaal te laten verlopen. Gedwongen door tekorten en pandemie, wordt er flink gesubsidieerd en geïnvesteerd in digitalisering binnen de zorg. Wet- en regelgeving is, niet geheel onlogisch, dus ook in ontwikkeling op dit vlak. Digitaal wordt soms zelfs verplicht gesteld, uiteraard kunnen kwaliteits- en veiligheidseisen dan niet uitblijven. ICTRecht neemt u daarom graag mee in de nieuwe wet- en regelgeving die in 2021 van toepassing is geworden en wat in 2022 verwacht kan worden voor de zorg op de onderwerpen ICT en privacy.

Strengere veiligheidseisen aan medische software

Terugkijkend op 2021 is de nieuwe regelgeving over medische hulpmiddelen, waaronder medische software, wellicht wel de grootste en belangrijkste update van het afgelopen jaar. Deze regelgeving volgt uit de Medical Device Regulation (MDR) en is sinds 26 mei 2021 van toepassing op de meeste medische hulpmiddelen en in-vitro diagnostiek. De MDR is een Europese verordening en hoeft dus niet in nationale wet- en/of regelgeving te worden omgezet. De MDR heeft de meeste impact op de fabrikanten van medische hulpmiddelen, maar er is ook een nieuwe rol voor zorginstellingen weggelegd. In de MDR staat de term 'medisch hulpmiddel' centraal. Dit is een hulpmiddel dat bedoeld is om te worden gebruikt voor een medisch doeleinde, zoals het diagnosticeren, voorspellen of behandelen van een ziekte, letsel of een beperking. De definitie is op een aantal punten uitgebreid, waardoor meer medische software als medisch hulpmiddel wordt aangemerkt. Bovendien zal medische software sneller in een hogere risicoklasse worden geplaatst, waardoor er ook strengere regels van toepassing zijn. Elk (medisch) hulpmiddel wordt namelijk door de MDR in een bepaalde risicoklasse ingedeeld (I, IIa, IIb en III).

Op het moment dat de fabrikant een medisch hulpmiddel op de markt wil brengen, is daarvoor een CE-markering nodig. Dit geeft aan dat het product voldoet aan de wettelijke veiligheids- en prestatie-eisen. De risicoklasse van het product bepaalt wie de CE-markering toekent. In de lagere risicoklassen is het mogelijk dat de fabrikant zelf vaststelt dat het medische hulpmiddel voldoet. Bij een hogere risicoklasse (waar onder andere medische software onder

valt) moet een Notified Body het product controleren of het veilig is en aan de wettelijke eisen voldoet.

Een ander belangrijk onderdeel van de nieuwe MDR is dat patiënten meer duidelijkheid krijgen. Deze duidelijkheid wordt verschaft door de Europese databank EUDAMED. In deze databank kunnen patiënten en zorgprofessionals informatie vinden over medische hulpmiddelen op de Europese markt.[1] De EUDAMED wordt gefaseerd beschikbaar. Op dit moment kunnen fabrikanten zichzelf en hun hulpmiddel registreren.

1. 'Wetgeving medische hulpmiddelen', rijksoverheid.nl.

Korte terugblik op nieuwe coronawetgeving

Behalve de MDR zijn er meer wetswijzigingen in het kader van zorg met een groot maatschappelijk belang in werking getreden. De Tijdelijke wet maatregelen Covid-19 is hier een goed voorbeeld van. Sinds de uitbraak van de coronacrisis hebben verschillende veiligheidsregio's op basis van noodverordeningen maatregelen kunnen nemen om de verspreiding van het virus te beperken. Noodverordeningen zijn echter bedoeld voor kortdurende (crisis)situaties. Omdat de coronacrisis langer duurt, was het nodig om de noodverordeningen te vervangen door de Tijdelijke wet maatregelen Covid-19.[2] De noodverordeningen bieden namelijk vanuit het oogpunt van democratische legitimatie een minder goede basis dan een wet in formele zin. Door deze wet is het mogelijk om flexibel coronamaatregelen te kunnen aanpassen, in te trekken of juist te nemen.[3] De wet is op 1 december 2020 in werking getreden.

2. Tijdelijke wet maatregelen Covid-19.
3. 'Coronawet vervangt noodverordeningen', rijksoverheid.nl.

Het invoeren van de coronatoegangsbewijzen is één van de genomen maatregelen, welke nu wettelijk verankerd is in de Tijdelijke wet coronatoegangsbewijzen. Hierin wordt bijvoorbeeld een uitzondering gemaakt op de wettelijke bewaartermijn voor het medisch dossier van 20 jaar. Een positieve Covid-19 uitslag en bijbehorend dossier dienen maximaal een jaar bewaard te worden, een negatieve uitslag en dossier maximaal vier weken. De termijn begint te lopen op het moment dat de test wordt afgenomen.

Bij het inrichten van de coronatoegangsbewijzen zijn verschillende privacyoverwegingen meegenomen. In het kader van dataminimalisatie ziet de afnemer via de CoronaCheck Scanner alleen de QR-code (niet waarop deze gebaseerd is: dubbele vaccinatie, negatieve PCR-test of herstelbewijs), initialen en geboortedatum van de aanbieder. Daarnaast worden de gegevens alleen lokaal opgeslagen, en bijvoorbeeld niet gedeeld met het Ministerie van VWS. Dit heeft op zijn beurt weer tot kritiek geleid, aangezien het hierdoor niet mogelijk is om QR-codes in te trekken van personen die reeds over een geldige QR-code beschikten maar toch positief worden getest.

Tot slot speelde er eind 2021 een discussie over de mogelijkheid tot het inzetten van het coronatoegangsbewijs op de werkvloer. De Autoriteit Persoonsgegevens (AP) was eind 2020 duidelijk in haar standpunt: een werknemer hoeft niet te vertellen of hij/zij wel of niet gevaccineerd is. Sterker nog, de werkgever mocht hier volgens de AP niet eens naar vragen. Waar deze wettelijke grondslag eerder voor horeca en sportwedstrijden is gecreëerd, werd hier expliciet in benoemd dat deze niet voor werkvloer geldt. Wanneer het kabinet doorzet met deze maatregel, dient deze wet hier dus op te worden aangepast. Dit blijft evenwel een lastige afweging voor het kabinet. Een werknemer heeft tenslotte geen vrije keuze om wel of niet naar het werk te gaan. Denk bijvoorbeeld aan docenten of artsen. Op het moment van schrijven wordt de wetgeving alvast voorbereid. Of hier een meerderheid voor in de Tweede en Eerste kamer komt, is lastig te zeggen.

De Wet digitale overheid is een terug- én vooruitblik

Een van de onderwerpen die niet alleen in 2021 een rol speelt, maar ook een belangrijke plek op de agenda van 2022 krijgt is de digitalisering van de overheid. Nederland digitaliseert, en ook de overheid moet hierin mee. De Wet digitale overheid (Wdo) is een logisch gevolg. Deze wet, op dit moment nog enkel wetsvoorstel, legt de basis voor de (verdere) digitalisering van de gemeenschappelijke infrastructuur van de overheid, zoals haar websites.

Deze wet komt niet uit de lucht vallen. Sinds 1 juli 2018 is namelijk al het Tijdelijk besluit digitale toegankelijkheid overheid van kracht.[4] Uit dit tijdelijke besluit volgt de wettelijke verplichting 'digitale toegankelijkheid overheid' die vanaf 23 september 2020 van kracht is. Dit besluit wordt daarom op termijn vervangen door de Wdo. Lees het artikel "Zorgaanbieder, kan uw patiënt al veilig inloggen?" over de impact van de Wdo op de zorg.

4. 'Bedenk dat je veel mensen uitsluit met een ontoegankelijke website', digitaleoverheid.nl.

Digitale communicatie tussen zorgaanbieders

Randvoorwaarde voor zorgverleners om goede zorg te verlenen is dat ze op het juiste moment beschikken over adequate, actuele en uniforme gegevens over de patiënt.[5] Door tijdige, elektronische uitwisseling van de juiste gegevens kan deze goede zorgverlening worden bevorderd.[6] Dit is aanleiding geweest voor het Wetsvoorstel Elektronische Gegevensuitwisseling in de Zorg (Wegiz).

Deze wet vormt de basis om bij Algemene Maatregel van Bestuur gegevensuitwisselingen aan te wijzen die ten minste elektronisch moeten plaatsvinden, met als uiteindelijke ambitie om te komen tot volledig gedigitaliseerde en gestandaardiseerde uitwisseling van gegevens. Eén van de speerpunten van de Wegiz is het creëren van optimale interoperabiliteit tussen de verschillende gebruikte systemen.

5. Kamerstukken II 2020/21, 35824, nr. 3, p. 1 (MvT).
6. Kamerstukken II 2020/21, 35824, nr. 3, p. 1 (MvT).

Belangrijk om op te merken is dat het wetsvoorstel geen verplichting tot het uitwisselen van gegevens oplegt (wel de verplichting dat als er uitgewisseld wordt door zorgaanbieders, dat dit dan op elektronische wijze gebeurt).[7] Eén van de zorgen die de Autoriteit Persoonsgegevens (AP) eerder over het wetsvoorstel heeft geuit, is namelijk dat een verplichte uitwisseling van gegevens mogelijk kan leiden tot een inbreuk op het medisch beroepsgeheim. Ook vanuit de Tweede Kamer zijn hierover meerdere vragen gesteld. Naar aanleiding van het advies van de AP en de vragen vanuit de Kamer is recent het wetsvoorstel op dit punt aangevuld en verduidelijkt.[8]

7. 'Gegevens uitwisselen in de zorg: net als sms', gegevensuitwisselingindezorg.nl.
8. 'Wetsvoorstel elektronische gegevensuitwisseling zorg: risico op aantasting medisch beroepsgeheim', autoriteitpersoonsgegevens.nl.

Het wetsvoorstel ligt nu bij de Tweede Kamer voor plenaire behandeling. De verwachting is dat deze behandeling in januari 2022 zal plaatsvinden en dat de eerste gegevensuitwisseling, als het wetsvoorstel wordt aangenomen, begin 2023 in werking zal treden.

Veldnorm medische kwaliteit van AI

De Europese regelgeving over AI (artificiële intelligentie) zal nog even op zich laten wachten. Omdat AI enorme potentie heeft en impact kan hebben op de kwaliteit van onze gezondheidszorg, wordt er nu een veldnorm "medische kwaliteit van AI" ontwikkeld. De veldnorm is een initiatief van het ministerie van VWS. De focus ligt op voorspellende AI-algoritmen (AIPA's) die onderdeel zouden kunnen worden van een hulpmiddel dat onder de MDR (Medical Device Regulation) valt. Eind 2021 wordt de veldnorm na een revisieronde in de praktijk getest, om te beoordelen wat de praktische toepasbaarheid is. In januari 2022 wordt verwacht dat de veldnorm beschikbaar wordt gesteld.

Per fase (er zijn er zes[9]) zijn er minimale eisen en aanbevelingen opgesteld door een werkgroep bestaande uit clinici, norm experts, epidemiologen, datamanagers, ethici, statistici, beleidsmedewerkers, kwaliteitsmedewerkers, data scientists en AI-experts werkzaam bij verschillende organisaties. De veldnorm zal relevant zijn voor toepassers, ontwikkelaars van AI, controlerende instanties en maatschappelijke partijen. En er wordt verwacht dat bij het gebruik van de veldnorm, het pas toe of leg uit regime zal worden toegepast.

9. https://bit.ly/3sWMjqS.

Er is bij het opstellen rekening gehouden met verschillende (deels overlappende) wettelijke kaders zoals de MDR en de Algemene verordening gegevensbescherming. Toepassers en ontwikkelaars worden meegenomen in hoe ze de wettelijke kaders moeten toepassen bij het gebruik en de ontwikkeling van medische AI.

Op de langere termijn: meer duidelijkheid in het sociale domein

Niet alleen direct na de jaarwisseling verandert er veel, ook op de lange termijn staat een aantal wetswijzigingen en nieuwe wetten op de planning. Eén van deze nieuwe wetten is de Wet aanpak meervoudige problematiek sociaal domein (Wams). Deze wet is het gevolg van de decentralisatie van taken uit het sociaal domein. Gemeenten zijn namelijk sinds 2015 verantwoordelijk voor een breed scala aan taken uit het sociaal domein, zoals jeugdzorg, werk, inkomen en zorg aan langdurig zieken. Deze taken zijn voor een groot deel overgenomen van de Rijksoverheid.[10] Een van de belangrijkste doelen van de decentralisatie is om burgers passende ondersteuning te kunnen bieden bij het vergroten van zelfredzaamheid en participatie.[11] De burgers die een beroep doen op ondersteuning bij taken uit het sociaal domein hebben vaak ondersteuning bij meervoudige problematiek nodig.[12]

Een blijvend probleem bij de aanpak van de meervoudige problematiek is de gegevensuitwisseling tussen de betrokken partijen. De AP heeft namelijk al aangekaart dat er geen overkoepelende wettelijke regeling is voor de domein overstijgende verwerking van persoonsgegevens in het sociaal domein.[13] Gemeenten kunnen gezien het feit dat een duidelijke grondslag ontbreekt, hun taak om domeinoverstijgend burgers te ondersteunen niet goed uitvoeren.[14] Vanuit het Programma Sociaal Domein is daarom het thematraject "Uitwisseling Persoonsgegevens en Privacy" (UPP) in gang gezet. In het traject wordt gewerkt aan het opheffen van 'wettelijke' knelpunten op het gebied van gegevensuitwisseling, die recht doet aan de privacy van mensen. Uit dit traject is het Wams voortgekomen. Deze wet moet regelen dat gemeenten in specifieke situaties de ruimte krijgen om te verkennen of sprake is van meervoudige problematiek en welke partijen nodig zijn om de problemen op te lossen, zodat snellere en meer gecoördineerde 'integrale' hulp mogelijk is.[15] De verwachting is dat deze wet eind 2022 in werking treedt.[16]

Innovatie in de zorg blijft doorgaan

2021 bracht voor de zorg de nodige nieuwe wet- en regelgeving met zich mee. Het steeds veranderende regelgevende kader zorgt ervoor dat innovatie in de zorg altijd door blijft gaan, maar dat de veiligheid van patiënten en andere burgers gewaarborgd blijft. Met het oog op 2022 zal dit niet anders zijn, gezien de plannen die nog op tafel liggen.

Wilt u op de hoogte blijven van nieuwe ontwikkelingen?

Word dan lid van onze LinkedIn community: https://www.linkedin.com/groups/12211946.

10. 'Decentralisatie van overheidstaken naar gemeenten', rijksoverheid.nl.
11. Kamerbrief over gegevensuitwisseling en privacy bij meervoudige problematiek, 27 september 2019, p.1, rijksoverheid.nl.
12. Kamerbrief over gegevensuitwisseling en privacy bij meervoudige problematiek, 27 september 2019, p.2, rijksoverheid.nl.
13. Onderzoeksrapport Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming, april 2016, p. 2, autoriteitpersoonsgegevens.nl.
14. Kamerbrief over gegevensuitwisseling en privacy bij meervoudige problematiek, 27 september 2019, p.2 en 3, rijksoverheid.nl.
15. 'Wetsvoorstel Aanpak meervoudige problematiek sociaal domein' (Wams), 19 maart 2020, programmasociaaldomein.nl.
16. 'Wetsvoorstel Aanpak meervoudige problematiek sociaal domein' (Wams), 19 maart 2020, programmasociaaldomein.nl.

Trainingsoverzicht Zorg & ICT

Wilt u zelf meer kennis in huis halen?
ICTRecht Academy biedt diverse praktische trainingen en webinars op het gebied van zorg & ICT.
De trainingen en webinars worden gegeven door onze eigen trainers uit het werkveld.

On demand webinars

Direct uw kennis over zorg & ICT vergroten? Met onze (gratis) zorg & ICT webinars bent u snel op de hoogte van de laatste ontwikkelingen.

Deze webinars vinden online plaats.
Lees meer!
https://bit.ly/3K1ppV7

Dinsdag 22 maart 2022

ICT & gezondheidsrecht (6 PO-punten)

Weten welke regels gelden bij het uitwisselen van medische gegevens online en hoe men moet werken in de cloud? Leer alles over ICT en gezondheidsrecht.

Deze training vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3qeroOc

Dinsdag 29 maart 2022

FG in de zorg(praktijk)

Tijdens deze training wordt ingegaan op de rol, werkzaamheden en bevoegdheden van de FG in de zorg in relatie tot de (privacy)wetgeving binnen de zorgsector.

Deze training vindt plaats in Utrecht.
Lees meer!
https://bit.ly/31NYVp5

Dinsdag 26 april 2022

FG zorg en informatiebeveiliging

Privacy en informatiebeveiliging zijn nauw met elkaar verbonden. Waartegen dient informatie te worden beschermd en wanneer zijn de maatregelen 'passend'?

Deze training vindt plaats in Utrecht.
Lees meer!
https://bit.ly/3fuaNzT

Donderdag 24 november 2022

Zorg op afstand (eHealth)

Leer in deze training over de vereiste juridische afspraken voor beeldschermzorg en hun aandachtspunten, inclusief de meest gehanteerde standaarddocumenten.

Deze training vindt plaats in Utrecht en online. Lees meer!
https://bit.ly/3JYNdsN

Donderdag 2 februari 2023

Privacy in de gezondheidszorg

Na deze training weet u wat de aandachtspunten zijn in de zorg voor de bescherming van medische persoonsgegevens en welke aanvullende regels er gelden.

Deze training vindt plaats in Utrecht en online. Lees meer!
https://bit.ly/3K1dw1D

ICTRECHT
academy

NEDERLANDSE ORDE VAN ADVOCATEN

iapp CPE credits approved

Donderdag 16 februari 2023

Security in de gezondheidszorg

Tijdens deze training wordt ingegaan op datalekken en informatiebeveiliging in de zorg. U leert o.a. beveiligingsincidenten te duiden als datalek (of niet).

Deze training vindt plaats in Utrecht en online. Lees meer!
https://bit.ly/3HVYuII

Donderdag 30 maart 2023

Elektronisch uitwisselen van medische gegevens: systemen in de zorg

Leer in deze training o.a. de ontwikkelingen op het gebied van wet- en regelgeving over het elektronisch uitwisselen van patiëntgegevens te duiden.

Deze training vindt plaats in Utrecht en online. Lees meer!
https://bit.ly/3HUpZCf

Heeft u vragen of wilt u meer weten?

Neem contact op met onze opleidingscoördinator Britt Telleman via e-mail: academy@ictrecht.nl of telefoonnummer: 020 663 19 41.

Britt Telleman
Opleidingscoördinator

ICTRECHT
adviesbureau

Meer informatie over hoe wij werken? Bezoek ictrecht.nl