Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2024–2025

27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

36 121 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de Europese ruimte voor gezondheidsgegevens

AI[1]

BRIEF VAN DE MINISTER VAN VOLKSGEZONDHEID, WELZIJN EN SPORT

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 7 april 2025

Om de zorg voor iedereen goed, toegankelijk en betaalbaar te houden, is de beweging ingezet van traditionele zorg naar passende (digitale en hybride) zorg, gezondheid en preventie. Digitalisering, gegevensuitwisseling en databeschikbaarheid vervullen hierin een cruciale rol. Met de Nationale Visie en Strategie (NVS) werken we aan databeschikbaarheid in 2035 voor burgers, zorgverleners en de wetenschap. Eerder ontving u de brief «agenda van databeschikbaarheid in de zorg» waarmee ik u hierover informeerde.[2]

De European Health Data Space-Verordening (EHDS) draagt bij aan betere zorg door betere databeschikbaarheid. Die elektronische uitwisseling is essentieel, en daarbij ook de zeggenschap die burgers over hun zorg- en persoonsgegevens kunnen uitoefenen. De EHDS geeft burgers een aantal rechten waarmee zij die zeggenschap kunnen vormgeven. Heel belangrijk daarbij zijn beperkingsrechten, zoals de «opt-out». In deze brief ga ik – zoals toegezegd tijdens het wetgevingsoverleg betreffende Verzamelwet gegevensverwerking VWS II.a van 27 januari 2025 – in op deze **beperkingsrechten** en mijn visie daarop.

Ik informeer u over de beperkingsrechten en de juridische, technische en praktische haalbaarheid om die in Nederland te implementeren. Ik schets de vervolgstappen voor een zorgvuldige implementatie. En ik doe drie andere toezeggingen uit het wetgevingsoverleg af.

Hoe zeggenschap in de zorg nu geregeld?

Bij zeggenschap van burgers in het kader van het beschikbaar stellen en het uitwisselen van persoonlijke (elektronische) gezondheidsgegevens

[1] De letters AI hebben alleen betrekking op 27 529.
[2] Kamerstukken I 2024/2025, 27 529.

kst-27529-AI
ISSN 0921 - 7371
's-Gravenhage 2025

voor primair gebruik en secundair gebruik, is op hoofdlijnen de volgende regelgeving van toepassing:

AVG en Uitvoeringswet AVG: de Nederlandse implementatie van de Europese Algemene Verordening Gegevensbescherming (AVG) waarin de grondslagen zijn opgenomen voor de verwerking van gegevens.
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz): hierin zijn regels opgenomen ten aanzien van het beschikbaar stellen en uitwisselen van gegevens via een zogenoemd «elektronisch uitwisselingssysteem». Met een «elektronisch uitwisselingssysteem» wordt gedoeld op «een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, zoals het Landelijk Schakelpunt (LSP).
Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) en de Wet Beroepen in de Individuele Gezondheidszorg (wet BIG): de nationale wetgeving waarin o.a. het medisch beroepsgeheim is geregeld. Hieronder wordt nader toegelicht wat het medisch beroepsgeheim inhoudt.

Medisch beroepsgeheim

De informatie die je met je arts of therapeut deelt, moet vertrouwelijk blijven en mag niet worden gedeeld met andere personen die niet betrokken zijn bij de behandeling. Dit heet het beroepsgeheim. In Nederland is dat wettelijk vastgelegd.[3] Het beroepsgeheim zorgt voor:
Onbelemmerde toegang tot de zorg: iedereen kan de hulp van een zorgverlener inroepen, zonder de zorg dat hun informatie beschikbaar komt bij anderen.
Beperken van zorgmijding: voorkomen dat mensen zorg mijden of onvolledige informatie geven omdat ze niet willen dat de gegevens door anderen dan hun zorgverlener worden ingezien.

Het beroepsgeheim is niet absoluut. Er zijn situaties waarin een arts het beroeps-geheim mag of moet doorbreken en gegevens mag of moet delen:
1. Met toestemming van de patiënt;
2. op basis van veronderstelde toestemming van de patiënt (bijvoorbeeld in acute zorg situaties);
3. bij een wettelijke plicht (zoals bijvoorbeeld de meldplichten in de Wet publieke gezondheid);
4. bij een conflict van plichten (bijvoorbeeld een ernstig dreigend gevaar voor anderen);
5. of een zwaarwegend belang (voor bijvoorbeeld nabestaanden).

Als wordt gewerkt met *elektronische uitwisselingssystemen* die de gegevens al van tevoren beschikbaar stellen, gelden aanvullende waarborgen ter bescherming van de privacy van de patiënt. Deze staan in Wabvpz. Het vooraf beschikbaar stellen via een elektronisch uitwisselingssysteem door de zorgverlener vereist op dit moment altijd uitdrukkelijke toestemming van de patiënt.[4] Op dit wettelijke vereiste van uitdrukkelijke toestemming bestaan géén uitzonderingen, het gaat hier strikt om een opt-in. Dat betekent dat er geen toestemming is voor het delen van gegevens, tenzij de burger dit aangeeft.
Het beroepsgeheim is er dus voor individuen, maar ook voor de maatschappij. Het richt zich daarbij op de relatie van patiënten met individuele beroepsbeoefenaren.

[3] Zie artikel 7:457 BW (WGBO), artikel 88 van de Wet BIG en 7.3.11 van de Jeugdwet.
[4] Artikel 15a lid 1 Wabvpz.

Het medisch beroepsgeheim mag worden doorbroken als een wettelijke plicht dit vereist of als de patiënt toestemming heeft gegeven. EHDS bevat zo'n wettelijke plicht. De EHDS zorgt daarmee voor een wijziging van het medisch beroepsgeheim zoals we dat nu in Nederland kennen.

Kortom: een burger moet in veel gevallen toestemming geven voor het (individueel) uitwisselen van persoonsgegevens, en altijd als dit via een elektronisch uitwisselingssysteem is. Dit geldt voor het delen van informatie tussen zorgverleners, bijvoorbeeld als iemand naar een ander ziekenhuis gaat. Maar ook voor het delen van informatie met anderen, bijvoorbeeld met wetenschappers die onderzoek willen doen.

Over de EHDS

Op 5 maart van dit jaar is de EHDS gepubliceerd in het Publicatieblad van de Europese Unie. Deze verordening heeft drie hoofddoelen:

1. **Databeschikbaarheid voor primair gebruik**
   De EHDS zorgt voor bredere beschikbaarheid van gezondheidsgegevens voor gebruik in het primair zorgproces. Daarbij krijgen burgers zeggenschap over gezondheidsgegevens en moeten zij hierin worden gefaciliteerd.
2. **Databeschikbaarheid voor secundair gebruik**
   De EHDS bevordert ook de beschikbaarheid van niet tot personen herleidbare gegevens voor secundaire doeleinden zoals onderzoek, beleid en innovatie.
3. **Regulering van de markt voor EPD-systemen.**[5]

Omdat de Tweede Kamer specifiek heeft gevraagd om een toelichting op opt-out-mogelijkheden bij de eerste twee doelen, zal ik mij in deze brief daarop richten. Het derde doel wordt in een Kamerbrief na de zomer beschreven.

Doelstelling van VWS

Het Ministerie van VWS zet zich in om Nederland gezond en vitaal te houden. Daarvoor is het essentieel dat zorgverleners beschikken over de juiste gegevens op de juiste plek om de meest passende zorg te kunnen verlenen. Daarin maakt de EHDS een grote slag. Ik juich deze ontwikkeling toe. Vanuit Nederland zijn we al enkele jaren bezig om dit doel te bereiken, bijvoorbeeld via de Wegiz. De EHDS versnelt dit proces. Daarnaast kan het volksgezondheidsbeleid, door de beschikbaarheid van gegevens voor secundair gebruik, meer effectief worden ontwikkeld.

Ik zie echter ook dat de EHDS gevolgen heeft voor hoe we in Nederland het medisch beroepsgeheim hebben ingericht. Om de nadelige gevolgen hiervan te ondervangen zijn aanvullende stappen nodig in wetgeving. Hierop kom ik verder in deze brief op terug.

Rechten voor zeggenschap over gegevens

De EHDS bevat diverse plichten voor zorgverleners om (persoons)gegevens van de patiënt toegankelijk te maken of te verstrekken aan derden, zoals andere zorgverleners. Tegelijkertijd geeft de EHDS burgers een aantal **beperkingsrechten** waarmee zij zeggenschap over hun persoonsgegevens kunnen uitoefenen, omdat zij daarmee op individueel niveau kunnen verhinderen dat gezondheidsgegevens beschikbaar worden gesteld en uitgewisseld.

---

[5] EPD staat voor elektronisch patiëntendossier.

Er zijn twee beperkingsrechten. Het eerste recht is het **recht op opt-out**, wat inhoudt dat betrokkenen kunnen verhinderen dat hun elektronische gezondheidsgegevens, in weerwil van de verplichting in de EHDS, door de zorgverlener beschikbaar worden gesteld voor andere zorgverleners. Het opt-out recht resulteert er dus in dat gegevens alleen beschikbaar blijven bij de zorgverlener waar je in behandeling bent en niet beschikbaar zijn voor derden. Het tweede recht is het **recht op toegangsbeperking van zorgverleners**. Dit recht geeft de mogelijkheid om beperkingen aan te brengen wie welke gegevens kan inzien. Dit vereist dus een technische functionaliteit om regie te houden op de inzagemogelijkheid van je gegevens door zorgverleners. Omdat deze rechten nauw met elkaar samenhangen en zij zich allebei richten op het beperken van toegang tot gegevens, zal ik ze in deze brief ook in samenhang bekijken en aanduiden.

Naar een nieuwe balans tussen privacy en efficiënt gegevensgebruik

Het is van belang dat privacy van de burgers wordt beschermd. Wat in de spreekkamer besproken wordt, moet in de spreekkamer blijven. De arts is daar ook toe verplicht (medisch beroepsgeheim). Het is daarom belangrijk dat burgers voldoende zeggenschap hebben over hen betreffende (gezondheids-)gegevens.

Naast het belang van bescherming van de privacy van burgers, is het ook van belang dat de juiste gegevens op de juiste plek beschikbaar zijn (data-beschikbaarheid). Dit draagt bij aan het verlenen van betere en snellere zorg aan patiënten. Zo kan ook efficiënter gewerkt worden en kunnen administratieve lasten verlaagd worden. Daarnaast helpt het in het voorkomen van (medische) fouten doordat gegevens niet overgenomen te hoeven worden van één systeem naar een ander systeem. Databeschikbaarheid kan daarnaast ook bijdragen aan wetenschappelijk onderzoek of de ontwikkeling van AI-oplossingen, die als hulpmiddel kunnen dienen tegen personeelstekorten in de zorg.

Een van de doelen van de EHDS is om databeschikbaarheid voor het leveren van zorg te verbeteren. Concreet betekent dit dat behandelende zorgverleners het recht krijgen om toegang te krijgen tot gegevens van hun patiënt op een gestandaardiseerde manier. Dit zorgt ervoor dat de arts beschikt over de juiste en meest actuele gegevens, waardoor onnodige behandelingen en onderzoeken kunnen worden voorkomen. Door nieuwe standaardisatieprocessen rondom toegang tot – en de registratie van – gezondheidsgegevens neemt bovendien de registratiedruk voor zorgverleners af. De EHDS zal dus leiden tot lagere kosten en administratieve lasten.

Naast betere zorg heeft de EHDS ook andere voordelen voor patiënten. Door de nieuwe regels voor gegevensregistratie kan de burger eenvoudiger beschikken over diens eigen gezondheidsgegevens, doordat deze op een centrale plek voor de burger inzichtelijk worden gemaakt. Daar kan hij dan bijvoorbeeld zien welke zorgverlener op welk moment bepaalde zorggegevens heeft opgevraagd. Op dit moment zijn deze gegevens in Nederland nog decentraal beschikbaar.

Ook onder de EHDS moeten zorgaanbieders het privacy-principe van dataminimalisatie blijven toepassen. Dat betekent dat zorgaanbieders alleen de gegevens van de patiënt in mogen zien die specifiek nodig zijn voor de behandeling.

De komst van de EHDS wijzigt het medisch beroepsgeheim niet, het fundamentele principe van vertrouwelijkheid blijft immers in stand. Wel zal met de komst van de EHDS de grondslag voor het doorbreken van het

beroepsgeheim bij elektronische gegevensuitwisseling veranderen. We gaan van een systeem van toestemming voordat gegevens elektronisch uitgewisseld worden, de opt-in-systematiek, naar een systeem met een wettelijke grondslag (de EHDS) die een opt-out-systematiek regelt. In deze nieuwe systematiek krijgt de zorgaanbieder ingevolge de EHDS de wettelijke verplichting om de digitale gezondheidsgegevens over zijn cliënt elektronisch beschikbaar te stellen aan andere zorgaanbieders van deze cliënt. De cliënt heeft vervolgens de mogelijkheid om dit middels zijn beperkingsrechten, ook wel de opt-out-systematiek genoemd, te voorkomen of hier grenzen aan te stellen. De opt-out-systematiek moet gelijke waarborgen bieden voor de burgers als de opt-in-systematiek.

Het beroepsgeheim in de zorg is een fundamenteel principe dat zorgverleners verplicht om medische en persoonlijke informatie van patiënten vertrouwelijk te behandelen. Patiënten moeten namelijk openlijk kunnen spreken over hun gezondheidsproblemen zonder angst dat hun informatie bij derden terechtkomt. Zonder een sterke vertrouwensband tussen patiënt en zorgverlener kan de kwaliteit van de zorg verminderen. In het ergste geval zou dat kunnen leiden tot zorgmijdend gedrag. De burger zal, ook na inwerkingtreding van de EHDS, dan ook de mogelijkheid krijgen om zijn beperkingswensen te registeren. Op welke wijze dit kan bespreek ik hieronder.

Beperkingsrechten bij primair gebruik

De EHDS biedt burgers twee beperkingsrechten: het **recht op een opt-out** en **het recht op toegangsbeperking**.

Recht op opt-out wordt in nationale wetgeving neergelegd

Of EU-lidstaten het recht op opt-out voor hun eigen burgers mogelijk willen maken, mogen ze zelf bepalen. Doen ze dit, dan moet dit recht in nationale wetgeving worden neergelegd. Ik heb u in juli 2024 al laten weten dat ik hier voor kies.[6]

Opt-out bij primair gebruik

Zorgaanbieders moeten toegang hebben tot de relevante en noodzakelijk persoonlijke elektronische gezondheidsgegevens van burgers die zij behandelen, ongeacht de lidstaat waar de zorgaanbieder gevestigd is of waar de behandeling plaatsvindt (art. 11 EHDS). Zorgverleners moeten dus de in de EHDS genoemde (persoons)gegevens toegankelijk maken voor andere zorgverleners. Op basis van de EHDS hebben burgers het recht om de toegang tot hun gezondheidsgegevens voor zorgaanbieders te beperken. Daarnaast hebben zij het recht om de uitwisseling van die gegevens met derden via de digitale toegangsdiensten tegen te houden (het recht op opt-out), indien en voor zover dat in nationale wetgeving is geregeld. Zoals ik uw Kamer eerder heb laten weten, wil ik van de mogelijkheid gebruikmaken om het opt-outrecht in nationale wetgeving te regelen.

Zoeken naar balans tussen gebruiksvriendelijkheid en functionaliteit

Bij de implementatie van de opt-out moet goed worden gekeken naar de technische, financiële en praktische haalbaarheid. Enerzijds is het essentieel dat burgers eenvoudig hun voorkeuren kunnen aangeven en begrijpen. Anderzijds vereisen complexe ICT-systemen veilige, toegankelijke en uniforme registraties, wat technische uitdagingen oplevert bij het

[6] *Kamerstukken II 2023/2024, 21 501-31 nr. 758.*

vormgeven van de opt-out. Het vinden van een balans tussen gebruiksvriendelijkheid en systeemfunctionaliteit is cruciaal, maar moeilijk, omdat flexibiliteit voor de burger niet altijd verenigbaar is met efficiënte gegevensverwerking.

Onderzoek naar technisch en praktische haalbaarheid van de opt-out

Juridisch gezien biedt de EHDS de ruimte om op verschillende gegevensniveaus een opt-out toe te passen. Op welk dataniveau er onderscheid kan worden gemaakt moet echter nog worden onderzocht. In het vervolgonderzoek zal ik kijken naar de technische, financiële en praktische mogelijkheden van onderscheid op dataniveau

Het is belangrijk dat de burger het heft in eigen handen kan nemen waarbij het wel belangrijk is dat de gegevens ook voor de zorgverleners bruikbaar blijven. Dit ga ik zorgvuldig uitzoeken en neem ik mee in de verdere uitwerking van de opt-out.

Daarnaast moet het voor burgers eenvoudig en voldoende begrijpelijk zijn om bezwaar te registreren. Dit betekent een balans vinden in genoeg keuzes voor de burger om het recht naar eigens wens te kunnen invullen, maar niet te ingewikkeld waardoor de consequenties van keuzes niet meer te overzien zijn. Ik wil het mogelijk maken dat de burger hier vol vertrouwen een overwogen en bewuste keuze in kan maken. Het risico in de balans tussen genoeg keuzemogelijkheden en voldoende begrijpelijk wordt ook door de Autoriteit Persoonsgegevens gezien.[7]

Ook hecht ik veel waarde aan het vertrouwen van de burger in het zorgsysteem als zijn privacy. De burger moet er zeker van zijn dat gegevens veilig worden verwerkt. Als dit vertrouwen hoog is, dan zal hij zijn beperkingsmogelijkheden proportioneel inzetten. Dit is goed voor zijn zorgverlener, maar ook bevorderlijk voor zijn zorgbehandeling. Om dit vertrouwen hoog te houden wil ik er daarom voor zorgen dat bij de implementatie van de beperkingsrechten de stem van de patiënt, en zijn doenvermogen, actief wordt meegenomen.

Daarom ga ik de komende periode met veldpartijen, zorgverleners en patiëntorganisaties in gesprek om te kijken wat de technische en praktische haalbaarheid is van de opt-out. Bij dit onderzoek is de zorgvuldige uitvoering van een mogelijke gelaagdheid een kernvraag. Daarbij wordt ook gekeken of het mogelijk is om de burger de keuze te geven om in acute zorgsituaties zijn gegevens wel beschikbaar te stellen. Verder wordt tijdens dit onderzoek onderzocht welke gevolgen de inzet van het opt-out-recht heeft voor de concernonderdelen van de overheid. Daarbij gaat het niet alleen om de onderdelen die vallen onder de reikwijdte van de EHDS (bijvoorbeeld bij het Rijksvaccinatieprogramma), maar ook de overdracht van gegevens vanuit de curatieve zorg naar Wmo-zorg.

Het recht op toegangsbeperking voor zorgverleners

Het recht op toegangsbeperking kan worden ingeroepen tegen de eigen zorgverlener. Dit betekent dat een zorgverlener niet in kennis wordt gesteld van de gegevens waarvoor de beperking geldt. Dat kan dus ook de behandelende zorgverlener zijn. Ik ga onderzoeken hoe dit vormgegeven kan worden zodat de burger haar rechten kan uitoefenen.

---

[7] *Position paper EHDS,* Autoriteit Persoonsgegevens, 12 maart 2025.

Van «grip door de patiënt» naar «grip door de burger»

Vanuit VWS zijn trajecten gestart om de patiënt meer mogelijkheden te geven om regie te kunnen voeren op zijn persoonsgegevens.

Nu kan de patiënt via volgjezorg.nl zien welke zorgverlener toegang heeft gekregen tot zijn persoonsgegevens. En via de centrale voorziening Mitz kan toestemming worden geregistreerd voor het elektronisch delen van gegevens tussen zorgverleners. Verder kan de patiënt – op grond van huidige wetgeving – zijn zorgverlener vragen om bepaalde medische gegevens niet te delen met andere zorgverleners. Hier moet gehoor aan worden gegeven, tenzij er zwaarwegende redenen zijn om dit niet te doen, bijvoorbeeld voor het declareren van de behandeling.

Onder de EHDS kan de burger al vóór en ná de behandeling zijn rechten inzetten om te bepalen *welke gegevens* voor *wie* beschikbaar worden gesteld. Deze beperkingskeuzes kunnen bij een publieke digitale voorziening worden geregistreerd.

Beperkingsrechten bij het secundair gebruik

Voordelen van databeschikbaarheid voor secundair gebruik

In de EHDS staat dat bepaalde datagebruikers – zoals onderzoekers en beleidsmakers – gebruik kunnen maken van gegevens die iets zeggen over algemene of individuele gezondheid. Deze gegevens worden dan, na een strenge vergunningsprocedure en niet-herleidbaar tot individuen, beschikbaar gesteld aan deze datagebruikers.

Deze nieuwe werkwijze biedt kansen voor de Nederlandse gezondheidszorg. Ik ondersteun om die reden dan ook het nut en de noodzaak van deze ontwikkeling. Door toegang tot gezondheidsgegevens kunnen (zorg)innovaties – zoals de toepassing van AI in de zorg – een impuls krijgen. Dit kan niet alleen bijdragen aan betere zorg, maar ook aan minder administratieve lasten voor zorgverleners. De voordelen zitten bijvoorbeeld in de schaalgrootte die mogelijk is door in de verschillende lidstaten via een vergelijkbare procedure data aan te kunnen vragen. Grotere datasets bieden betere mogelijkheden voor onderzoeken en zeker ook voor de mogelijkheden om AI goed te trainen en ontwikkelen. Deze AI kan dan bijvoorbeeld weer ingezet worden om administratieve taken over te nemen van zorgverleners. Daarnaast kan de overheid bijvoorbeeld de beschikbare data gebruiken om gerichter beleid te maken. Dit leidt tot effectiever zorgbeleid en zorgt dat publiek geld voor gezondheidszorg efficiënter kan worden besteed.

Opt-out bij secundair gebruik

Burgers kunnen rechtstreeks een beroep doen op het EHDS-opt-out-recht bij secundair gebruik. De manier waarop burgers dit recht feitelijk kunnen uitoefenen moet wel worden uitgewerkt. De geregistreerde opt-out met betrekking tot het beschikbaar stellen van elektronische gezondheidsgegevens voor secundair gebruik geldt in beginsel voor alle in de EHDS genoemde gegevens die voor dat doel kunnen worden gebruikt. Lidstaten mogen daarnaast regels maken voor aanvullende waarborgen bij specifiek gevoelige gegevens.

Aanvullende waarborgen voor specifiek gevoelige gegevens

De EHDS maakt het verder mogelijk om bij de beschikbaarstelling van specifiek gevoelige gezondheidsgegevens *aanvullende waarborgen* te stellen. Dat kan bij:
- Genetische gegevens
- Biobankgegevens
- Gegevens uit wellness-apps

Wat er wordt bedoeld met «aanvullende waarborgen» kan op verschillende manieren worden geïnterpreteerd. Zo zegt de EHDS niets over de mogelijkheid om gelaagdheid aan te brengen op gegevensniveau of onderzoeksdoel. Dat betekent echter ook niet dat de verordening dat niét toelaat. Op dit moment doe ik verder onderzoek over hoe deze «aanvullende waarborgen» kunnen worden geïnterpreteerd op een wijze die in lijn is met de EHDS. Bij dit onderzoek kijk ik ook naar de mogelijkheid of een selectieve opt-out mogelijk is. Dit geldt dan mogelijk voor bepaalde specifieke gezondheidgegevens of gegevens die worden gebruikt in het publieke belang (bijvoorbeeld bij de bestrijding van een levensbedreigende infectieziekte of bij onderzoek naar zeer zeldzame aandoeningen). Ook kijk ik of het mogelijk is om toestemming te vragen voor het verwerken van deze specifieke zeer gevoelige gegevens.

Bij dit onderzoek wordt ook gekeken naar de technische, financiële en praktische haalbaarheid van deze aanvullende waarborgen in combinatie met de beperkingsrechten. Voor DNA-gegevens en biobankgegevens is nu al duidelijk welke uitgangspunten ik belangrijk vind. Hieronder ga ik daar verder op in.

Burger mag geen nadeel ondervinden van hergebruik DNA-gegevens

Sommige genetische gegevens zijn bijzonder en het is belangrijk om deze goed te beschermen en zeggenschap van burgers te waarborgen. In de Nederlandse (gezondheids)onderzoekspraktijk wordt dit momenteel ook zo gezien. De gedragscode Gezondheidsonderzoek van COREON wordt hier uitgebreid op ingegaan.[8] Daarin wordt «onderzoek met gegevens die intrinsiek herleidbaar worden geacht, zoals bij «whole genome sequencing», en waarbij deze gegevens breder worden gedeeld dan binnen de onderzoekinstelling», aangemerkt als onderzoek met bijzondere privacyrisico's of consequenties voor de donor. Hiervoor is volgens de bestaande gedragscode in beginsel apart toestemming voor nodig.

Onder genetische gegevens valt ook data die van zichzelf al te weinig informatie bevat om herleidbaar te zijn tot individuen. Zo is bij de analyse van bijvoorbeeld alleen een kankercel het risico op herleidbaarheid beperkt. En dat terwijl zulke gegevens steeds belangrijker worden voor wetenschappelijk onderzoek. Ik zie daarom de voordelen van hergebruik van dit soort gegevens, maar vind ook dat deze voordelen niet mogen doorslaan in het nadeel van de burger.

Mijn ambtsvoorganger heeft aan u gemeld dat er vanwege de maatschappelijke perspectieven en publieke waarden rondom DNA-technologie, samen met burgers en professionals overheidsbeleid hierover moet worden ontwikkeld.[9] In opdracht van ZonMW is in 2024 advies uitgebracht over hoe deze partijen bij dit beleidsproces betrokken kunnen worden.[10]

---

[8] *Gedragscode gezondheidsonderzoek,* COREON, januari 2022, paragraaf 4.4.3, p. 57.
[9] *Kamerstukken II, 2023/2024, 30 793 nr. 703 .*
[10] *Publieke waarden en perspectieven ten aanzien van DNA-technologie voor zorg en preventie,* Schuttelaar & Partners, i.o.v. ZonMw, Den Haag, september 2024.

Deze adviezen worden meegenomen in de gesprekken die ik wil doen met veldpartijen, zorgverleners en patiëntorganisaties.

Tijdens het wetgevingsoverleg rond Verzamelwet IIa stelde uw Kamer een aantal vragen waarop ik toezegde later uitgebreider terug te komen. Het ging om vragen rond de verantwoordelijkheidsverdeling en invulling van de beveiliging van patiëntgegevens, autorisatievraagstukken door meer personen en Vektis en de beveiliging.

Cybersecurity

Bij deze ga ik in op de toezegging om meer uitleg te geven over informatiebeveiliging binnen de context van gegevensverwerking en welke ondersteuning ik op dit vlak aan zorgaanbieders biedt.

Goede informatiebeveiliging in de zorg is ontzettend belangrijk omdat het hier gaat over het beschermen van patiëntgegevens en de continuïteit van zorg. De verantwoordelijkheid hiervoor ligt primair bij zorgaanbieders. Deze aanbieders richten naar aard van organisatie/zorgprocessen en hun mogelijkheden deze beveiliging op verschillen de manieren in. Hier geldt dat maatwerk de norm is. In de aanpak van dit maatwerk zijn er echter wel zorgbrede elementen te onderscheiden. De aanpak is genormeerd in de NEN 7510. De NEN-7510 schrijft onder andere voor dat zorginstellingen de risico's voor informatiebeveiliging in kaart brengen en hiervoor passende maatregelen nemen. De norm vereist ook beheersmaatregelen voor de bescherming van netwerken, bedrijfscontinuïteit en bereikbaarheid. De IGJ ziet toe op naleving van de NEN-7510 norm.

Ik bied op verschillende manieren ondersteuning om de zorg digitaal weerbaarder te maken Ten eerste ondersteun ik financieel het cybersecurity expertisecentrum in de zorg, Z-CERT. Z-CERT voorziet zorgaanbieders van advies en dreigingsinformatie, en kan tevens netwerken monitoren op kwetsbaarheden of verdachte activiteiten. In het geval van een incident kan Z-CERT een zorgaanbieder ondersteunen bij het verhelpen van de gevolgen van een cyberaanval. Ik stuur aan op het beheerst groeien en verbreden van Z-CERT door aansluiting van meer zorginstellingen en uitbreiding van het dienstenaanbod. Ik zet ook in op meer bewustwording van de cyberrisico's in de zorg met het Actieplan Informatieveilig Gedrag. Driekwart van de datalekken in de zorg kent immers een gedragscomponent.

Daarnaast werk ik aan de doorontwikkeling van (wettelijke verplichte) informatiebeveiligingsnormen in de zorg, waaronder de genoemde basis norm NEN7510 en de daaruit voortvloeiende normen voor gegevensuitwisseling (NEN7512) en logging (NEN7513). Momenteel wordt de Europese NIS2-richtlijn geïmplementeerd in de Cyberbeveiligingswet. Deze richtlijn heeft tot doel om de digitale weerbaarheid van essentiële en belangrijke entiteiten, waaronder de organisaties in de zorg, naar een hoger gemeenschappelijk niveau te brengen. Zorginstellingen krijgen onder Cbw een zorgplicht, wat betekent dat zij aan moeten tonen dat hun informatie- en veiligheidssystemen goed functioneren en dat ze maatregelen nemen om risico's op digitale aanvallen te verkleinen. Daarnaast gaat er een meldingsplicht gelden voor ernstige cyberincidenten. Expertisecentrum Z-CERT krijgt onder de Cbw een wettelijke taak en meer middelen om zorgorganisaties te ondersteunen en monitoren.

Ten slotte zet ik in op versterking van toezicht en handhaving door de IGJ. De IGJ houdt toezicht op informatiebeveiliging bij zorgaanbieders en gaat daarbij uit van de eerdergenoemde wettelijk verplichte NEN-norm 7510. De IGJ voert steekproefsgewijs controles uit op naleving van de norm.

Uit inspectiebezoeken in voorgaande jaren blijkt dat in diverse zorgsectoren de naleving van de NEN7510 te wensen overlaat. Ik vind dit zorgelijk. De IGJ heeft hierover diverse keren in factsheets naar het veld gecommuniceerd[11]. Uit de toezichtsresultaten blijkt dat niet alle zorgaanbieders die zij hebben bezocht – zoals de ziekenhuizen, ZBC's/particuliere klinieken en aanbieders in de gehandicaptenzorg – aantoonbaar voldoen aan de NEN7510. De IGJ ziet vaak een combinatie aan oorzaken waarop de naleving tekort schiet. Voorbeelden hiervan zijn het ontbreken van voldoende bewustzijn op het onderwerp informatiebeveiliging en het gebrek aan prioritering van voldoende middelen (tijd, geld en expertise) voor het onderwerp. Wanneer de naleving op de NEN7510 te wensen overlaat, vraagt de IGJ om verbeterplannen met termijnen. Ziekenhuizen hebben tijdens dit verbetertraject een flinke inhaalslag gemaakt. Eind 2023 is gecommuniceerd dat het merendeel voldoen aan de NEN7510.[12]
Om zorginstellingen te ondersteunen bij het voldoen aan de NEN7510 norm, heb ik de NEN opdracht gegeven implementatietools te ontwikkelen. De implementatiehandvatten, zoals bijvoorbeeld een e-learning ter introductie, worden in 2025 kosteloos beschikbaar gesteld. De tools zijn nuttig voor zowel organisaties die voor het eerst de NEN7510 implementeren als voor organisaties die NEN7510 al hebben geïmplementeerd en moeten overstappen op de nieuwe versie van de genoemde norm.

Autorisatie van behandelteams voor het verwerken van gezondheidsgegevens

Het lid Tielen beschreef tijdens het wetgevingsdebat dat zij tijdens werkbezoeken vaak hoort van zorgprofessionals en onderzoekers dat gegevens voor zowel wetenschappelijk onderzoek alsook voor patiëntgerichte diagnostiek en behandeling makkelijker beschikbaar zouden moeten zijn. De huidige wetten en regels zouden dit verhinderen. Een verpleegkundig specialist die zelf grafiekjes moest maken ten behoeve van de behandeling en spiegelinformatie, en dit niet door de doktersassistente liet doen omdat dan heel vaak toestemming gevraagd moet worden. Het lid Tielen vroeg zich hierbij af in een soort brainstormidee af of een soort teamlicentie mogelijk zou zijn, zodat een behandelteam met de data aan de slag kan gaan. Hieronder geef ik mijn reactie hierop.

Het recht laat meer ruimte toe om zorggegevens te verwerken dan uit bovenstaand situatieschets. Ter verduidelijking van het juridische kader rondom de verwerking van gezondheidsgegevens in de zorg leg ik uit waar rechtmatige gegevensverwerking in de zorg aan moet voldoen, als er geen sprake is van uitdrukkelijke toestemming.

Autorisatie bij primair gebruik

Zorgaanbieders mogen gezondheidsgegevens verwerken als dat nodig is voor de zorgverlening aan patiënten, maar ook voor het beheer van de instelling, bijvoorbeeld de financiële administratie van de zorgverlening en interne kwaliteitsborging (artikel 9, tweede lid onder J AVG, ander uitgewerkt onder artikel 30, derde lid, onder A UAVG). Zorgaanbieders mogen gezondheidsgegevens verwerken als dat nodig is voor de uitvoering van de geneeskundige behandelingsovereenkomst die zij met de patiënt hebben (art. 6 lid 1 onder b AVG). Dat geldt ook voor de

---

[11] Zie Onderwerpen I E-health I Inspectie Gezondheidszorg en Jeugd (ioi.n1); sectoren: ziekenhuizen, zelfstandige klinieken, ggz, gehandicaptenzorg, verpleeghuiszorg, thuiszorg, eerstelijnszorg, jeugd.

[12] Ziekenhuizen maken stevige inhaalslag met informatiebeveiliging I Publicatie I Inspectie Gezondheidszorg en Jeugd.

medewerkers die rechtstreeks bij dezelfde behandelovereenkomst zijn betrokken.

Ook de invulling van het medisch beroepsgeheim wordt als drempel ervaren bij het delen van gegevens. Het medisch beroepsgeheim in Nederland gaat ervan uit dat de medische beroepsbeoefenaar geen gezondheidsgegevens aan derden mag geven, tenzij de betrokken patiënt daar toestemming voor heeft gegeven. Dit geldt niet voor anderen die rechtstreeks bij de behandeling zijn betrokkenen, zoals doktersassistenten (artikel 7:457 BW (onderdeel van de WGBO)).

In aanvulling hierop moeten zorgaanbieders organisatorische en technische maatregelen treffen ter beveiliging en bescherming van persoonsgegevens. Zorgaanbieders moeten in dat kader voldoen aan informatiebeveiligingsnormen, zoals in het bijzonder de NEN7510. Onderdeel daarvan is dat wordt gewaarborgd dat alleen die medewerkers toegang tot medische dossiers krijgen als dat nodig is voor de behandeling van de patiënt. Dat moet gebeuren door middel van een autorisatiebeleid en logging (inclusief de controle op logging). Autorisatie en toegangsverlening kan plaatsvinden op het niveau van functie of rol van de medewerker.

Kortom, in het voorbeeld van het lid Tielen is het alleszins acceptabel dat de desbetreffende assistente (als onderdeel van het behandelteam) zonder toestemming van de patiënt toegang heeft tot de relevante gegevens, voor zover dat nodig is voor de behandeling van de patiënt of het monitoren van de kwaliteit van de zorgverlening.

Autorisatie bij Secundair gebruik

Onderzoekers en andere secundaire datagebruikers krijgen niet zomaar toegang tot gezondheidsgegevens. Voordat toegang gegeven wordt tot een dataset vindt in de meeste gevallen een beoordelingsprocedure van de betrokken instellingen en/of dataverstrekkers plaats. Bij deze beoordeling wordt onder andere gekeken naar de juridische grondslagen, de opzet van de verwerking en de informatiebeveiliging. De procedures die daarvoor gebruikt worden zijn niet altijd gelijk. Voor WMO-plichtig onderzoek is bijvoorbeeld medisch-ethische toetsing door een erkende medisch-ethische toetsingscommissie (METC) verplicht. Voor niet WMO-plichtig onderzoek geldt deze verplichting niet.

Bij secundair gebruik met gezondheidsgegevens dient in de meeste gevallen ook een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA) plaats te vinden. In de DPIA wordt onder andere vastgelegd welke gegevens worden verwerkt, voor welk doel deze worden verwerkt, welke juridische grondslagen van toepassing zijn, in hoeverre de verwerking noodzakelijk en proportioneel is, of er minder ingrijpende alternatieven zijn, wat de risico's zijn en hoe deze risico beheerst kunnen worden.

Wanneer uit de beoordelingsprocedures en DPIA blijkt dat de gegevens veilig verwerkt kunnen worden, worden gegevens beschikbaar gemaakt voor secundair gebruik. Daarbij is het uiteraard zaak dat alleen onderzoekers en onderzoeksondersteuners (zoals datamanagers en ICT-ers) die noodzakelijkerwijs betrokken zijn bij de gegevensverwerking toegang krijgen tot de gegevens. Personen die ondersteunende rollen hebben ten aanzien van het secundair gebruik kunnen dus onder voorwaarden toegang krijgen. Daarbij is het wel belangrijk dat waarborgen met betrekking tot bijvoorbeeld geheimhouding zijn vastgelegd. Het is de verantwoordelijkheid van de gegevensverwerker om rollen en toegangs-

rechten toe te wijzen. De gedragscode gezondheidsonderzoek van Coreon[13] staat hoe instellingen de toegangsbeveiliging kunnen invullen. Daarbij wordt geadviseerd om zoveel mogelijk aan te sluiten bij de eerder genoemde NEN norm omtrent gegevens, NEN7510.

Het is voor het zorgveld van belang dat zij het juridisch kader op een goede wijze interpreteren. Veel van de veronderstelde juridische belemmeringen komen voort uit een onjuiste interpretatie van de regels. Ik hoop met mijn beantwoorden een deel van de onduidelijkheid weg te kunnen nemen. Op dit moment voorzie ik dus geen directe aanleiding om wetgeving te wijzigen.

Vektis

Hierbij kom ik terug op mijn toezegging tijdens het wetgevingsoverleg Verzamelwet gegevensverwerking VWS II.a[14] om in te gaan op de ondergrens van tien patiënten en cliënten bij de verwerking van gegevens door Vektis.[15]

Vektis geeft aan geen rapporten op te stellen met gegevens die direct of indirect naar personen te herleiden zijn en zegt altijd te controleren op potentiële herleidbaarheid, rekening houdend met de aard van de informatie. Vektis streeft naar de balans tussen zo min mogelijk informatieverlies (groepen in beeld brengen) en tegelijk het waarborgen van hun anonimiteit. Vektis heeft de ervaring dat deze balans in de regel ligt bij een ondergrens van 10 personen. Als uitgangspunt neemt Vektis in rapportages dan ook geen gegevens op die betrekking hebben op minder dan 10 personen. Daarbij maakt Vektis onderscheid tussen «nul personen» en «weinig personen» (minder dan 10). Vektis rapporteert zodoende of er sprake is van 0 personen, minder dan 10 personen, of 10 of meer personen, waarbij alleen in het laatste geval een getal wordt weergegeven. Over een (sub)groep kleiner dan 10 personen doet Vektis geen nadere uitspraken.

Tot slot

Elektronische gegevensuitwisseling en databeschikbaarheid blijven een complex vraagstuk. De Nationale visie en strategie wijst het zorgveld hierbij de weg en werkende landelijke oplossingen komen steeds dichterbij. Toch kost dit proces tijd.
We doen er alles aan om tot een goede, vlotte, maar ook zorgvuldige en veilige implementatie van gegevensuitwisseling te komen.

De Minister van Volksgezondheid, Welzijn en Sport,
M-F. Agema

---

[13] Coreon, Commissie Regelgeving Onderzoek, Gedragscode gezondheidsonderzoek, januari 2022

[14] *Kamerstukken II 2024/25, 36 579 nr. 11.*

[15] Zorgverzekeraars en Wlz-uitvoerders zijn verwerkingsverantwoordelijken voor de verzekerden- en declaratiegegevens waarover zij beschikken. Vektis treedt namens en in opdracht van zorgverzekeraars en Wlz-uitvoerders op als verwerker van deze gegevens voor de uitvoering van een aantal (wettelijke) taken.