

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

BBB-fractie

D66-fractie

ChristenUnie-fractie

JA21-fractie

II. Reactie van de minister

I. Vragen en opmerkingen vanuit de fracties

Vragen van de leden van de fractie van de BBB:

De leden van de BBB-fractie vragen waarom de kosten zo hoog zijn. Is dat om leveranciers te helpen of komt er een eigen Rijksvoorziening? Als dat laatste het geval is, wie of wat zal daar dan de regie over gaan voeren?

Daarnaast valt het de leden van de fractie van de BBB op dat er wel over 'logging' wordt gesproken, maar niet over 'monitoring'. Zij wijzen erop dat monitoring onder de Algemene verordening gegevensbescherming (AVG) verplicht is om misbruik te voorkomen.

Vragen van de leden van de fractie van D66:

De lidstaten krijgen de mogelijkheid om op basis van nationale wetgeving aan burgers het recht van opt-out toe te kennen. De leden van de D66-fractie vragen of de opt-out mogelijkheid standaard wordt opgenomen. Is de opt-out mogelijkheid voor Nederland een gangbare route, mede gezien de deskundigenbijeenkomst die destijds in de Eerste Kamer is gehouden² en het mondeling overleg op 7 juni 2023 waarin bleek dat een meerderheid van partijen vaststelden dat dit de sterke voorkeur heeft. Ook de minister⁴ heeft in dat overleg letterlijk gezegd: "we moeten er op de een of andere manier voor zorgen dat er zo'n opt-out in de acute zorg komt." Wat is de stand van zaken in dezen?

Daarnaast hebben de leden van de D66-fractie nog enkele vragen ten aanzien van de bescherming van het medisch beroepsgeheim. Betekent dit dat medische gegevens niet (kunnen) worden gedeeld? Vanuit het perspectief van patiënt en zorgverlener om tijdig hoogwaardige zorg te kunnen leveren, is het essentieel dat deze wel worden gedeeld. Wat wordt er feitelijk gedeeld?

Vragen van de leden van de fractie van de ChristenUnie:

In de brief schrijft u dat nader moet worden onderzocht of burgers bij het zogeheten 'recht van opt-out' onderscheid kunnen maken tussen nationale en Europese digitale zorgdossiers. Op welke termijn denkt u helderheid te kunnen verschaffen over de haalbaarheid van die mogelijkheid? En hoe beoordeelt u het Europese krachtenveld als het gaat over dit onderscheid bij opt-out, met name nu blijkt dat de Commissie en het Parlement daarvan geen voorstander zijn?

Bij het toestaan van inzage van gegevens door zorgverleners wordt de mogelijkheid geboden om onderscheid te maken tussen nationale zorgverleners en zorgverleners elders in Europa. Hoe beoordeelt u deze mogelijkheid? Hebben burgers daarmee voldoende controle over de toegang tot hun medische gegevens of blijft een opt-out op Europees niveau wenselijk?

De leden van de ChristenUnie-fractie stellen vast dat toegang tot persoonlijke gezondheidsgegevens in de gehele keten wordt vastgelegd ('gelogd'). In de EHDS wordt

aanvullend verplicht dat zulke log-gegevens inzichtelijk worden gemaakt voor de betreffende burger. Is het de bedoeling dat dit passief gebeurt, zodat de burger op eigen initiatief dient na te gaan wie wanneer welke gegevens heeft opgevraagd of gebeurt dit inzichtelijk maken actief, zodat de burger bijvoorbeeld een melding kan krijgen wanneer zijn of haar gegevens bevestigd zijn?

In algemene zin vragen deze leden hoe u de veiligheid beoordeelt van een veelomvattende database als deze met vertrouwelijke gegevens, zeker in tijden van digitale dreiging en cybercriminaliteit? Hoe wordt voorkomen dat de database wordt platgelegd door criminelen of statelijke actoren en hoe wordt verhinderd dat dergelijke partijen toegang krijgen tot de medische gegevens van burgers?

Vragen van de leden van de fractie van JA21:

Hoe groot en impactvol is volgens u het probleem dat de EHDS denkt op te lossen? Oftewel: hoeveel patiënten en hoeveel procent van het totaal aantal patiënten beweegt zich over de landsgrenzen heen voor acute zorgvragen?

Wegen de implementatielasten en -kosten op tegen de winst (bijvoorbeeld uitgedrukt in Quality's: Quality-adjusted life years) die gewonnen worden met de implementatie van EHDS?

Hoe verhoudt de EHDS zich volgens u tot de Wet elektronische gegevensuitwisseling in de zorg (Wegiz)?

Dwingt EHDS ook een standaardisatie af van medische coderingen, zoals SNOMED-CT? Zo nee, is dat niet wenselijk voor de interoperabiliteit tussen aanbieders en systemen?

De leden van de fractie van JA21 zien graag toegelicht wie de kosten draagt voor compliance aan EHDS?

II. Reactie van de minister

De leden van de fractie van de BBB vragen waarom de kosten zo hoog zijn. Zij vragen of dat is om leveranciers te helpen of dat er een eigen Rijksvoorziening komt.

De EHDS-verordening regelt een juridisch kader waarmee specifieke categorieën data beschikbaar moeten worden gesteld voor primair of secundair gebruik. Bij primair gebruik dient de data op een geharmoniseerde wijze te worden aangeleverd. Daartoe worden strikte eisen gesteld voor Elektronische Patiëntendossier systemen (EPD-systemen) zodat data ook daadwerkelijk interoperabel beschikbaar kan worden gesteld. De aanlevering van de data gebeurt vanuit de nationale zorginformatiestelsels waar de lidstaten zelf over gaan. Daarnaast vereist de EHDS-verordening de oprichting en aanwijzing van een aantal publieke entiteiten die naast toezichthoudende taken ook specifieke uitvoerende taken dienen uit te voeren.

In de financiële impactanalyse worden de totale investeringskosten weergegeven die nodig zijn om volledig te kunnen voldoen aan de verplichtingen uit de EHDS-verordening. Dit betreffen kosten bij zorgaanbieders om hun gegevens gereed te maken voor het beschikbaar stellen, of EPD-leveranciers die hun producten moeten aanpassen naar de vereisten uit de EHDS-verordening zodat deze op de markt mogen worden aangeboden. Daarnaast worden ook de kosten voor de overheid opgenomen zoals het aanwijzen/opzetten van de verplichte publieke entiteiten. Bij de weergave van de investeringskosten moet worden opgemerkt dat ook de kosten worden meegenomen die betrekking hebben op reeds lopende nationale beleidstrajecten zoals de kosten voor een landelijk dekkend netwerk van infrastructures, de verdere implementatie van de Wegiz, en de kosten voor de ontwikkeling van generieke functies. Deze nationale initiatieven zijn hierin opgenomen, omdat met de uitrol en verdere ontwikkeling daarvan Nederland ook aan de EHDS-verordening zou voldoen.

Overigens is de laatste update van de financiële impactanalyse gebaseerd op het Raadsmandaat van 5 december 2023. Ondertussen is er een politiek akkoord bereikt op de EHDS-verordening waarover ik u in mijn brief van 21 maart jl. heb geïnformeerd. Ik ben voornemens om nogmaals een update te laten uitvoeren op de financiële impactanalyse op basis van het politiek akkoord op de EHDS-verordening. Het eindrapport daarover zal ik aan beide Kamers toesturen zodra deze gereed is.

De leden van de fractie van de BBB vragen of, als dat laatste het geval is, wie of wat daar dan de regie over zal gaan voeren.

De kosten geven een breed overzicht weer van de investeringen die in Nederland moeten worden gedaan om aan de EHDS-verordening te voldoen. Hierin worden ook de kosten meegenomen die reeds zijn voorzien voor lopende nationale beleidstrajecten. Er zal nog een update worden uitgevoerd op de laatste financiële impactanalyse op basis van het politiek akkoord. Het eindrapport daarover zal ik aan beide Kamers toesturen zodra deze gereed is.

Daarnaast merken de leden van de fractie van de BBB op dat het hen opvalt dat er wel over 'logging' wordt gesproken, maar niet over 'monitoring'. Zij wijzen erop dat monitoring onder de Algemene verordening gegevensbescherming (AVG) verplicht is om misbruik te voorkomen.

Logging is een beveiligingsmaatregel waarbij wordt geregistreerd wie toegang heeft gehad tot persoonsgegevens. Ik veronderstel dat de BBB-fractie met de term 'monitoring' bedoelt dat regelmatig (al dan niet automatisch) moet worden gecontroleerd of er onregelmatigheden in de logbestanden voorkomen, zodat deze tijdig kunnen worden ontdekt en passende maatregelen kunnen worden genomen. De AVG bevat geen letterlijke verplichting om te loggen en/of te monitoren. Wel zijn logging en het regelmatig controleren van logbestanden in de meeste gevallen noodzakelijke beveiligingsmaatregelen om misbruik van persoonsgegevens te voorkomen. Op grond van de AVG moeten verwerkingsverantwoordelijken passende maatregelen nemen om persoonsgegevens te beveiligen, zodat het risico op misbruik van persoonsgegevens wordt geminimaliseerd. Op basis van deze algemene beveiligingsnorm zijn in de praktijk informatiebeveiligingsnormen, zoals NEN-normen, tot stand gekomen. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de algemene beveiligingsnorm uit de AVG en de daarmee samenhangende informatiebeveiligingsnormen. In de zorgsector is logging en het controleren van de logbestanden wel verplicht, op grond van het Besluit elektronische gegevensuitwisseling door zorgaanbieders, en – in het verlengde daarvan – de informatiebeveiligingsnorm NEN7513. De EHDS-verordening doet aan al deze verplichtingen niet af.

De leden van de fractie van D66 geven aan dat de lidstaten de mogelijkheid krijgen om op basis van nationale wetgeving aan burgers het recht van opt-out toe te kennen. Zij vragen of de opt-out mogelijkheid standaard wordt opgenomen.

De EHDS-verordening biedt lidstaten de mogelijkheid om (in nationaal recht) burgers het recht toe te kennen bezwaar te maken tegen het beschikbaar stellen van persoonlijke elektronische gezondheidsgegevens via digitale toegangsdiensten voor de levering van zorg (opt-out primair gebruik). Bij primair gebruik gaat het om het gebruik van (bijzondere) persoonsgegevens in het kader van de zorgverlening aan de patiënt. Een dergelijke opt-out regeling zal bestaan naast het – rechtstreeks uit het EHDS-voorstel voortvloeiende – recht van burgers om de toegang tot hun gegevens door zorgprofessionals en zorgaanbieders te kunnen beperken¹.

Voor secundair gebruik bepaalt de EHDS-verordening rechtstreeks dat burgers bezwaar kunnen maken tegen het verwerken van gegevens voor secundaire gebruiksdoeleinden (opt-out secundair gebruik). Onder strikte voorwaarden kan dit opt-out recht worden ingeperkt in het geval van doeleinden die betrekking hebben op het algemeen belang. Een inperking van het opt-out recht voor secundair gebruik moet altijd in nationale wetgeving worden vastgelegd en te worden genotificeerd bij de Europese Commissie.

Bij de implementatie van de EHDS-verordening in Nederland kijk ik uiteraard naar de belangen van databeschikbaarheid terwijl de privacy en de vrije toegang tot de zorg goed blijven geborgd. Bezien moet worden hoe invulling kan worden gegeven aan de nationale ruimte die de EHDS-verordening biedt rondom de verschillende opt-outs.

¹ De door de cliënt opgelegde beperkingen van toegang tot gezondheidsgegevens kunnen worden doorbroken als er sprake is van een situatie van vitaal belang bij de patiënt, bijvoorbeeld in levensbedreigende situaties.

De leden van de fractie van D66 vragen verder of de opt-out mogelijkheid voor Nederland een gangbare route is, mede gezien de deskundigenbijeenkomst die destijds in de Eerste Kamer is gehouden² en het mondeling overleg op 7 juni 2022³ waarin bleek dat een meerderheid van partijen vaststelden dat dit de sterke voorkeur heeft.

De EHDS-verordening biedt lidstaten de mogelijkheid voor een opt-out bij primair gebruik. Dit is een optie die ik serieus wil onderzoeken. Bij de vraag of een dergelijke opt-out wenselijk is, spelen verschillende aspecten een rol. Het is belangrijk dat er een goede balans wordt gevonden tussen databeschikbaarheid dat bijdraagt aan zorgontwikkeling aan de ene kant en het belang van privacy en (daarmee samenhangend) de vrije toegang tot de zorg die geborgd moeten blijven. Daarnaast moet in de afweging ook het door de EHDS-verordening gecreëerd recht van burgers op het beperken van de toegang voor de zorgverlener worden meegenomen. Bovendien moet ook rekening worden gehouden met de wijze waarop burgers dergelijke rechten straks kunnen uitoefenen. Tot slot is het belangrijk rekening te houden met het effect van de wijze waarop een opt-out regeling wordt vormgegeven op het vertrouwen van burgers in het beschikbaar stellen van hun persoonlijke elektronische gezondheidsgegevens voor primair en secundair gebruik. Hierbij zal ik analyseren hoeveel nationale ruimte de EHDS-verordening biedt om de vormgeving van de opt-out regeling zo veel mogelijk te aan laten sluiten op de nationale behoeften. Bij de overwegingen rondom een opt-out regeling betrek ik uiteraard de (eerdere) inbreng van veldpartijen en beide Kamers der Staten-Generaal.

De leden van de fractie van D66 merken op dat in de deskundigenbijeenkomst de toenmalige minister in dat overleg letterlijk heeft gezegd: "we moeten er op de een of andere manier voor zorgen dat er zo'n opt-out in de acute zorg komt." Zij vragen wat de stand van zaken in dezen is.

De beschikbaarheid van gegevens bij acute zorg moet snel worden verbeterd. Hier zet ik mij onverkort voor in. Het wetsvoorstel opvraagbaarheid gegevens acute zorg (Wogaz) lijkt inhoudelijk voor een groot deel te overlappen met de EHDS-verordening die naar verwachting dit najaar wordt bekrachtigd. Ik analyseer op dit moment wat de EHDS-verordening betekent voor het Wogaz-voorstel. Mijn voornemen is om beide Kamers der Staten-Generaal in het najaar, zodra de EHDS-verordening definitief is bekrachtigd, verder te informeren over de aanpassing van grondslagen voor gegevensuitwisseling in de acute zorg.

Daarnaast hebben de leden van de fractie van D66 nog enkele vragen ten aanzien van de bescherming van het medisch beroepsgeheim. Zij vragen of dit betekent dat medische gegevens niet (kunnen) worden gedeeld.

Het uitgangspunt van de EHDS-verordening is dat specifieke categorieën gegevens beschikbaar moeten worden gesteld zodat betere en snellere zorg kan worden geleverd. Daarnaast draagt het o.a. bij aan medisch-wetenschappelijk onderzoek en innovatie, zodat verbeterde en nieuwe behandelmethoden kunnen worden ontwikkeld. Databeschikbaarheid op grond van de EHDS-verordening gaat echter gepaard met een breed scala aan waarborgen zodat dit op een verantwoorde en transparante wijze gebeurt.

Voor het beschikbaar stellen van data bepaalt de EHDS-verordening dat zorgprofessionals toegang moeten kunnen krijgen tot persoonlijke elektronische gezondheidsgegevens die betrekking hebben op personen die zij behandelen. Dit houdt in dat de gegevenshouders (andere zorgaanbieders) deze gegevens beschikbaar moeten stellen zodat ook de behandelende arts de zorg kan leveren, ongeacht in welke EU-lidstaat die behandelend arts zich bevindt. De EHDS verplicht zorgaanbieders om (onder bepaalde omstandigheden en voorwaarden) patiëntgegevens uit medische dossiers te verstrekken. Dat komt neer op een wettelijke doorbreking van het medisch beroepsgeheim van de zorgaanbieder.

² Deskundigenbijeenkomst 'Gegevensuitwisseling in de zorg' d.d. 12 oktober 2021 (Kamerstukken I 2021/22, 31.765/27.529/35.824, J).

³ Mondeling overleg 'Gegevensuitwisseling in de zorg' met minister Kuipers (Kamerstukken I 2021/22, 27.529/35.824, T, blz. 13).

Verder moeten gegevens die zich bevinden bij zorgaanbieders ook (onder bepaalde voorwaarden) beschikbaar worden gesteld voor afgebakende zorggerelateerde doelen van secundair datagebruik, zoals medisch-wetenschappelijk onderzoek of innovatie. Het verplicht beschikbaar stellen van gegevens door gegevenshouders voor secundair gebruik mag pas plaatsvinden onder strikte voorwaarden. Een dergelijke verplichting tot het verstrekken van gezondheidsgegevens is pas aan de orde als een (nog op te richten) instantie voor toegang tot gezondheidsgegevens (Health Data Access Body, HDAB) daartoe een vergunning heeft verleend. De aanvrager van zo'n vergunning moet onder meer aantonen dat de gegevens noodzakelijk zijn voor de doelen die zijn genoemd in de EHDS en dat de aanvraag tevens voldoet aan de eisen die de EHDS daaraan stelt. Lidstaten kunnen ervoor kiezen om in dat kader ook een medisch-ethische toets verplicht te stellen. Daarnaast worden de gegevens alleen beschikbaar gesteld in een beveiligde verwerkingsomgeving en kan de gebruiker alleen met anonieme of onder strikte voorwaarden gepseudonimiseerde gegevens werken. De bedoeling is dat gegevensgebruikers alleen toegang hebben tot gegevens die niet herleidbaar zijn tot individuen.

De verplichting voor zorgprofessionals om gegevens beschikbaar te stellen voor primair en secundair gebruik betekent dat zij niet aan hun cliënten toestemming hoeven te vragen. Patiënten houden echter wel zeggenschap over hun gegevens doordat ze bezwaar kunnen maken tegen (bepaalde) verwerkingen van hun gegevens (opt-out). Hierdoor kunnen zorgprofessionals –zoals in de huidige praktijk ook vaak gebeurt– samen met de patiënt bepalen of het wenselijk is om gegevens beschikbaar te stellen.

De leden van de fractie van D66 merken op dat het vanuit het perspectief van patiënt en zorgverlener om tijdig hoogwaardige zorg te kunnen leveren, het essentieel is dat deze wel worden gedeeld. Zij vragen wat er feitelijk wordt gedeeld.

Ik ben het eens de leden van de D66 fractie dat databeschikbaarheid bij kan dragen aan het leveren van tijdige hoogwaardige zorg aan de patiënt. Op Europees niveau is daarom bepaald dat het belangrijk is dat bepaalde specifieke categorieën persoonlijke elektronische gezondheidsgegevens beschikbaar moeten worden gesteld. Dit heeft geleid tot het benoemen van zes prioritaire categorieën persoonlijke elektronische gezondheidsgegevens in de EHDS-verordening. Het gaat daarbij om:

- patiëntsamenvattingen;
- elektronische medicatie recepten
- elektronische verstrekkingen (van medicatie);
- medische beelden en verslagen daarover;
- laboratoriumresultaten; en
- ontslagverslagen.

Lidstaten hebben de bevoegdheid om te bepalen dat ook andere persoonlijke elektronische gezondheidsgegevens onder dit recht en daarmee de plicht komen te vallen. Ik ben voornemens te bezien of dit wenselijk is. Daarbij betrek ik uiteraard de inbreng van veldpartijen en beide Kamers der Staten-Generaal.

De leden van de fractie van de ChristenUnie geven aan dat in de brief staat dat nader moet worden onderzocht of burgers bij het zogeheten 'recht van opt-out' onderscheid kunnen maken tussen nationale en Europese digitale zorgdossiers. Deze leden vragen op welke termijn helderheid verschaft kan worden over de haalbaarheid van die mogelijkheid.

Het politieke akkoord op de EHDS-verordening is pas recentelijk bereikt. De verordening is daarmee ook nog niet definitief vastgesteld. De verwachting is dat dit in het vierde kwartaal van dit jaar zal gebeuren. De komende periode zal ik wel de impact van de EHDS-verordening voor Nederland alvast verder in kaart brengen. Daarin zal ik ook de implementatiemogelijkheden van het opt-out recht voor primair gebruik meenemen. Daarbij moet ook in kaart worden gebracht wat beleidsmatig wenselijk is zodat het past in de nationale context. Beide Kamers der Staten-Generaal zal ik informeren over de impact zo snel mogelijk nadat de verordening definitief is vastgesteld.

De leden van de fractie van de ChristenUnie vragen verder hoe ik het Europese krachtenveld beoordeel als het gaat over dit onderscheid bij opt-out, met name nu blijkt dat de Commissie en het Parlement daarvan geen voorstander zijn.

Onder de lidstaten is er brede steun voor de mogelijkheid voor burgers om bij het opt-out recht een onderscheid te maken tussen nationale en grensoverschrijdende beschikbaarheid van gegevens. De mogelijkheid voor een dergelijk onderscheid was daarom ook expliciet opgenomen in het Raadsmandaat van 5 december 2023. Echter, zowel het Europees Parlement als de Europese Commissie hebben gedurende de trilogonderhandelingen grote bezwaren geuit tegen een onderscheid tussen nationale en grensoverschrijdende beschikbaarheid. Daarbij is aangevoerd dat wanneer burgers bij toepassing van de opt-out onderscheid kunnen maken tussen lidstaten, dit mogelijk het onderlinge vertrouwen tussen lidstaten in het veilig en verantwoord omgaan met persoonlijke elektronische gezondheidsgegevens schaadt. Om die reden heeft de expliciete mogelijkheid om een onderscheid te maken het niet gehaald in het politiek akkoord over de EHDS-verordening. Maar omdat de huidige tekst het ook niet expliciet verbiedt dat een dergelijk onderscheid wordt gemaakt, zal ik nader laten onderzoeken welke ruimte nationaal mogelijk is bij de implementatie van een eventuele opt-out voor primair gebruik.

De leden van de fractie van de ChristenUnie merken op dat bij het toestaan van inzage van gegevens door zorgverleners de mogelijkheid wordt geboden om onderscheid te maken tussen nationale zorgverleners en zorgverleners elders in Europa. Deze leden vragen hoe deze mogelijkheid wordt beoordeeld.

De EHDS-verordening geeft expliciet aan dat burgers het recht krijgen om de toegang (inzage) tot delen of alle persoonlijke gezondheidsgegevens die vallen binnen de scope van de EHDS-verordening door zorgverleners of aanbieder te beperken. Het is de verantwoordelijkheid van de lidstaten om hun burgers te faciliteren zodat zij deze rechten kunnen uitoefenen. Lidstaten krijgen hierin een zekere mate van nationale ruimte bij de implementatie van deze rechten.

Aan de Commissie is gevraagd hoe zij tegen dit vraagstuk aankijkt. Daarop heeft de Commissie geantwoord dat zij zich een implementatie kan voorstellen waarbij het voor burgers mogelijk wordt gemaakt om in hun keuze een onderscheid te maken tussen nationale zorgverleners en aanbieders in andere EU-landen. Hoe exact vorm wordt gegeven aan dit recht in de Nederlandse implementatie ben ik aan het onderzoeken.

De leden van de fractie van de ChristenUnie vragen of burgers daarmee voldoende controle hebben over de toegang tot hun medische gegevens of dat een opt-out op Europees niveau wenselijk blijft.

De EHDS-verordening biedt lidstaten de mogelijkheid om via nationale wetgeving burgers het recht toe te kennen bezwaar te maken tegen het beschikbaar stellen van persoonlijke elektronische gezondheidsgegevens via zogenoemde digitale diensten voor toegang tot elektronische gezondheidsgegevens voor de levering van zorg (opt-out primair gebruik). Dit is een optie die ik serieus wil onderzoeken. Het is belangrijk om bij de uitwerking en concretisering van deze rechten rekening te houden met de wijze waarop de burger dit recht concreet kan uitoefenen. Bij de overwegingen daarover betrek ik uiteraard de inbreng van veldpartijen en beide Kamers der Staten-Generaal.

Sommige rechten op opt-out zijn in de verordening zelf opgenomen en behoeven daarom geen nadere uitwerking in nationale wetgeving. Bij secundair gebruik is het opt-out recht op Europees niveau vastgelegd, zodat dat recht rechtstreeks doorwerkt in het rechtstelsel van de lidstaten en burgers rechtstreeks een beroep kunnen doen op dat recht. Daarnaast krijgen burgers ook het recht om de toegang voor de zorgverlener tot de gezondheidsgegevens te beperken (bij primair gebruik). Ook dat recht is in de verordening zelf opgenomen, zodat burgers rechtstreeks een beroep kunnen doen op dat recht.

Los hiervan bevat de EHDS ten aanzien van primair gebruik van elektronische gezondheidsgegevens een aantal nieuwe rechten van burgers, waarmee zij in staat zijn regie en controle te hebben op gegevens die op hen betrekking hebben. Daaronder valt bijvoorbeeld een specifiek recht op inzage in medische dossiers en het recht op dataportabiliteit.

De leden van de fractie van de ChristenUnie stellen vast dat toegang tot persoonlijke gezondheidsgegevens in de gehele keten wordt vastgelegd ('gelogd'). In de EHDS-verordening wordt aanvullend verplicht dat zulke log-gegevens inzichtelijk worden gemaakt voor de betreffende burger. Deze leden vragen of het de bedoeling is dat dit passief gebeurt, zodat de burger op eigen initiatief dient na te gaan wie wanneer welke gegevens heeft opgevraagd of dat dit inzichtelijk maken actief gebeurt, zodat de burger bijvoorbeeld een melding kan krijgen wanneer zijn of haar gegevens bevestigd zijn.

De EHDS-verordening bepaalt dat burgers het recht hebben om informatie te verkrijgen van iedere toegang tot persoonlijke elektronische gezondheidsgegevens via de toegangsdienst voor zorgprofessionals in het kader van gezondheidszorg. Volgens de EHDS-verordening kan dit via automatische notificatie, maar wordt dit niet verplicht. Op dit moment onderzoek ik op welke wijze dit recht van burgers kan worden vormgegeven. Daarin is automatische notificatie een optie die ik serieus meeneem.

De leden van de fractie van de ChristenUnie vragen verder in algemene zin hoe ik de veiligheid beoordeel van een veelomvattende database als deze met vertrouwelijke gegevens, zeker in tijden van digitale dreiging en cybercriminaliteit.

Naar mijn oordeel geeft de EHDS-verordening een helder kader voor veilige en verantwoorde databeschikbaarheid en gegevensuitwisseling. Bovendien zullen de beginselen van gegevensbescherming uit de AVG en beveiligingsvereisten uit andere wet- en regelgeving van toepassing zijn.

In de context van primair gebruik worden lidstaten via het nationaal contactpunt voor eHealth (NCPeH) aangesloten op het MyHealth@EU infrastructuur. MyHealth@EU maakt gebruik van een digitale infrastructuur die losstaat van het reguliere internet. Op deze wijze wordt zoveel mogelijk voorkomen dat hackers en cybercriminelen via het reguliere internet toegang kunnen krijgen tot vertrouwelijke gegevens. Daarnaast dient iedere NCPeH voordat deze wordt aangesloten een uitgebreide audit van de Commissie te doorlopen. Daarin is veiligheid een belangrijk aspect waarop wordt gecontroleerd. Audits vinden ook na aansluiting plaats met enige regelmaat om compliance aan de veiligheidsvereisten te waarborgen.

De werkwijze voor secundair gebruik binnen de context van de EHDS is in lijn met het beginsel van dataminimalisatie en doelbinding uit de AVG. Er wordt dan ook een strenge controle toegepast op toegang tot de gegevens voor secundair gebruik. Persoonlijke elektronische gezondheidsgegevens blijven in beginsel bij de bron (de gegevenshouder). Enkel de nodige gegevens worden beschikbaar gesteld door de gegevenshouder aan de Nederlandse instantie voor toegang tot gezondheidsgegevens (ook wel Health Data Access Body – HDAB) als deze instantie een vergunning heeft verleend aan een gegevensgebruiker. Vervolgens krijgt de gegevensgebruiker uitsluitend toegang tot de gegevens in geanonimiseerde vorm of, waar strikt noodzakelijk, in gepseudonimiseerde vorm in een beveiligde verwerkingsomgeving. Een beveiligde verwerkingsomgeving bevat daarom alleen maar gegevens die nodig zijn voor de verwerking zoals in de vergunning bepaald. De HDAB verzamelt en beheert dus enkel tijdelijk persoonlijke elektronische gezondheidsgegevens die voor een specifieke vergunning nodig zijn. Binnen 6 maanden na afloop van de vergunning worden die gegevens gewist.

Wanneer een gegevensgebruiker toegang wil krijgen tot de gegevens in de beveiligde verwerkingsomgeving, dan wordt de gebruiker altijd geïdentificeerd en geautoriseerd. Op deze manier wordt gewaarborgd dat alleen gebruikers die genoemd staan in de vergunning toegang krijgen. Daarnaast worden de activiteiten gelogd voor monitoring zodat de verwerkingen op de data plaatsvinden conform wat in de vergunning staat en binnen de kaders van de EHDS. Gegevens blijven in beginsel altijd in de beveiligde verwerkingsomgeving. Alleen wanneer de HDAB kan verifiëren dat de data volledig anoniem is en niet te herleiden is tot een persoon kan de data eventueel worden gedownload. Doordat het volledig anonieme data betreft dient daar verder ook geen toezicht op te worden gehouden. Verder is de HDAB verantwoordelijk voor het toezicht op, en het auditen van, de beveiligde verwerkingsomgeving. De details rondom deze werkwijze en de benodigde technologie worden nog verder uitgewerkt, op Europees niveau en binnen het Nederlandse programma HDAB-NL. In deze uitwerking neem ik de reeds geldende wet- en regelgeving voor informatieveiligheid alsook nieuwe technologische ontwikkelingen mee. Onderdeel

hiervan zijn de wettelijk verplichte NEN-normen 7510, 7512 en 7513 voor informatiebeveiliging in de zorg.

Tot slot, de EHDS-verordening voorziet niet in een alomvattende database. Bij primair gebruik wordt er gewerkt aan een decentraal infrastructuur genaamd MyHealth@EU die databronnen op een veilige manier verbindt zodat gegevens kunnen worden uitgewisseld wanneer dat nodig is. Bij secundair gebruik zal binnen de beveiligde verwerkingsomgeving anonieme of pseudonieme data tijdelijk worden opgeslagen. Hieraan worden strikte eisen gesteld en gebeurt dit altijd onder toezicht van de HDAB.

Daarnaast vragen leden van de fractie van de ChristenUnie hoe voorkomen wordt dat de database wordt platgelegd door criminelen of statelijke actoren en hoe verhinderd wordt dat dergelijke partijen toegang krijgen tot de medische gegevens van burgers.

Voor het grensoverschrijdend uitwisselen van gegevens voor primair gebruik moeten lidstaten een Nationaal Contactpunt voor eHealth (NCPeH) opzetten die in verbinding staat met het MyHealth@EU infrastructuur. Deze infrastructuur maakt gebruik van een beveiligde digitale verbinding genaamd TESTA (Trans European Services for Telematics between Administrations) die volledig losstaat van het reguliere internet waardoor het buiten het bereik van criminelen of statelijke actoren blijft. Het is een infrastructuur die reeds gebruikt wordt voor het veilig verzenden van berichten en data tussen overheden in de EU en de Europese Commissie. Daarnaast is de uitwisseling tussen de NCPeH's altijd end-to-end encrypted. Bovendien gelden de hoogste privacy en gegevensbeveiligingsvereisten voor aansluiting van een NCPeH op MyHealth@EU. Voordat een NCPeH wordt aangesloten vindt er eerst een uitgebreide audit plaats door de Europese Commissie. Na aansluiting vinden reguliere audits plaats om ervoor te zorgen dat de NCPeH's nog steeds aan de vereisten voldoen.

Bij secundair gebruik blijven de gegevens in beginsel bij de bron en wordt toegang enkel verleend tot de nodige gegevens in een separate beveiligde verwerkingsomgeving. Dit is een maatregel om gegevensbescherming te waarborgen alsook om te voorkomen dat een zogenoemde single-point-of-failure ontstaat. Het doel daarvan is om te voorkomen dat criminelen of statelijke actoren via de infrastructuur van een HDAB en een beveiligde verwerkingsomgeving toegang krijgen tot de systemen van de gegevenshouders, zoals ziekenhuizen, en ze ook niet via deze route kunnen platleggen.

Ook de beveiligde verwerkingsomgeving wordt beschermd. Gebruikers van de beveiligde verwerkingsomgeving worden geïdentificeerd en geautoriseerd en activiteiten worden gelogd voor monitoring. Verder moet een beveiligde verwerkingsomgeving het risico minimaliseren van het onrechtmatig lezen, kopiëren, wijzigen of weghalen van elektronische gezondheidsgegevens met behulp van geavanceerde technologische middelen. Deze gegevens worden tijdelijk in de beveiligde verwerkingsomgeving opgeslagen en gehost. Het doel is om te voorkomen dat criminelen of statelijke actoren toegang krijgen of de systemen van een beveiligde verwerkingsomgeving kunnen platleggen. De details rondom deze werkwijze en de benodigde technologie worden nog verder uitgewerkt, op Europees niveau en binnen het Nederlandse programma HDAB-NL. In deze uitwerking neem ik de reeds geldende wet- en regelgeving voor informatieveiligheid alsook nieuwe technologische ontwikkelingen mee.

De leden van de fractie van JA21 vragen hoe groot en impactvol het probleem is dat de EHDS-verordening denkt op te lossen. Oftewel: hoeveel patiënten en hoeveel procent van het totaal aantal patiënten beweegt zich over de landsgrenzen heen voor acute zorgvragen?

Ik heb op het moment geen exacte cijfers over de het aantal patiënten dat zich over de landsgrenzen beweegt voor acute zorgvragen. Over het algemeen gaan burgers niet voor acute zorg naar het buitenland, deze acute zorgvraag overkomt een burger, zo ook als deze in het buitenland is.

Maar ik verwacht dat de impact van de EHDS-verordening op het gebied van primair gebruik aanzienlijk zal zijn. Steeds meer Nederlandse burgers wonen in een ander EU-lidstaat, dat aantal is in de afgelopen 20 jaar bijna verdubbeld naar ruim 600.000 in 2022. Dat is 3.6% van alle Nederlanders. Het gaat dan vooral om landen die grenzen aan Nederland en landen in Midden- en

Zuid-Europa⁴. Bovendien reizen burgers ook voor werk en vakantie naar het buitenland en wonen veel burgers in een Nederlandse grensregio waardoor zorg soms over de grens wordt verleend. Tot slot komen ook veel burgers van andere EU-lidstaten in Nederland.

Bij al deze burgers kan een zorgbehoefte optreden in een ander land dan hun woonland. De meest recente gegevens dateren uit 2014, waarin 1% van de Nederlanders behoefte had aan geplande zorg over de grens en 2% ongeplande zorg⁵. Ook de cijfers over de (gedeclearde) zorgkosten op basis van de Zorgverzekeringswet (Zvw) bij grensoverschrijdende zorg bieden inzicht. In 2022 ging het om een bedrag van zo'n 800 miljoen Euro⁶.

Naast het belang van de EHDS voor de grensoverschrijdende beschikbaarheid van gegevens voor primair gebruik, zijn er ook grote voordelen voor medisch-wetenschappelijk onderzoek en innovatie (secundair gebruik). Doordat datasets met anonieme of pseudonieme gegevens ook grensoverschrijdend beschikbaar kunnen worden gesteld voor secundair gebruik, kan er sneller onderzoek worden gedaan naar nieuwe behandelmethoden of medicaties.

De leden van de fractie van JA21 vragen ook of de implementatielasten en -kosten opwegen tegen de winst (bijvoorbeeld uitgedrukt in Quality's: Quality-adjusted life years) die gewonnen worden met de implementatie van EHDS-verordening.

Het doel van de EHDS-verordening is dat data beter beschikbaar komt voor de levering van zorg en ook medisch wetenschappelijk onderzoek, innovatie en beleid. Een paar concrete voorbeelden waar de EHDS-verordening een bijdrage aan kan leveren zijn als volgt:

- Als het gaat om de databeschikbaarheid voor primair gebruik, dan zie ik grote voordelen voor Nederlanders die bijvoorbeeld op vakantie een hartaanval krijgen. Bij een hartaanval telt iedere seconde. Als een arts in een ander EU-land dan toegang heeft tot de medische gegevens van deze patiënt, dan kan de arts inzien welke medicatie de patiënt gebruikt en of er al eerder hartaanvallen hebben plaatsgevonden. Kostbare tijd wordt bespaard en onnodig onderzoek voorkomen. Maar daarnaast gaat het ook veel kunnen betekenen voor Nederlanders die in de grensregio wonen en dagelijks de grens oversteken voor bijv. werk. Deze personen kunnen er gerust op zijn dat belangrijke medische gegevens toegankelijk zijn wanneer dat nodig is.
- Bij secundair gebruik kan gedacht worden aan onderzoek naar zeldzame ziekten. Door de zeldzaamheid van deze ziekten zijn datasets van alleen Nederlanders niet voldoende om goed onderzoek hierop te doen. Voor medisch-wetenschappelijk onderzoek is het essentieel voldoende gegevens te hebben om goede conclusies te trekken. Doordat soortgelijke datasets uit andere EU-landen ook beschikbaar komen, kan daardoor beter en sneller onderzoek worden gedaan naar bijvoorbeeld nieuwe behandelmethoden. Dit is een grote winst voor Nederland en de EU aangezien 1 op de 12 personen in de EU lijdt aan een zeldzame ziekte.

De EHDS-verordening zal de nodige investeringen vragen om aan de verplichtingen te voldoen. Echter, zoals ik al in de beantwoording van vraag 1 heb aangegeven wordt in de weergave van de investeringskosten ook de kosten meegenomen die betrekking hebben op reeds lopende nationale beleidstrajecten zoals de kosten voor een landelijk dekkend netwerk van infrastructuren, de verdere implementatie van de Wegiz, en de kosten voor de ontwikkeling van generieke functies. Deze nationale initiatieven zijn hierin opgenomen, omdat met de uitrol en verdere ontwikkeling daarvan Nederland ook aan de EHDS-verordening zal kunnen voldoen.

⁴ Peter Ekamper (2023), Nederlanders elders in Europa. *Demos: bulletin over bevolking en samenleving* 39 (7): 8. (ook gepubliceerd in het Financieel Dagblad van 4 september 2023).

⁵ Speciale Eurobarometer 425: Rechten van patiënten bij grensoverschrijdende gezondheidszorg in de Europese Unie: https://data.europa.eu/data/datasets/s2034_82_2_425_eng?locale=nl

⁶ Zorgcijferdatabank, Totale zorgkosten Zorgverzekeringswet. Grensoverschrijdende zorg: https://www.zorgcijfersdatabank.nl/databank?infotype=zvw&label=00-totaal&tabel=B_kost&qeq=j2022NEW&item=215

Verder vragen de leden van de fractie van JA21 hoe de EHDS-verordening zich verhoudt tot de Wet elektronische gegevensuitwisseling in de zorg (Wegiz)?

De Wegiz en de EHDS-verordening kennen veelal dezelfde uitgangspunten, namelijk het per specifieke gegevensuitwisseling toewerken naar verplichte interoperabiliteit. Onder interoperabiliteit wordt verstaan: de mogelijkheid om gegevens (van een specifieke gegevensuitwisseling) elektronisch en gestandaardiseerd uit te wisselen tussen alle zorgaanbieders in Nederland of Europa.

De essentie van de Wegiz en de EHDS-verordening komt overeen. De Wegiz loopt vooruit op de EHDS-verordening en helpt het Nederlandse zorgveld met het tijdig voldoen aan de verplichtingen van deze verordening.

Ondanks dat de EHDS-verordening en de Wegiz dezelfde uitgangspunten hebben, zal de EHDS-verordening impact hebben op de Wegiz, doordat de EHDS-verordening op onderdelen een andere opzet heeft om het doel te bereiken, namelijk het interoperabel uitwisselbaar maken van gegevens zodat sneller en betere zorg kan worden geleverd aan burgers. Ik onderzoek momenteel deze impact en blijf me inzetten om de EHDS- beleidskeuzes en de Wegiz-uitwerking parallel te laten lopen zodat het veld bij de inwerkingtreding van de specifieke gegevensuitwisselingen van de EHDS-verordening gereed is.

Ook vragen de leden van de fractie van JA21 of de EHDS-verordening ook een standaardisatie van medische coderingen afdwingt, zoals SNOMED-CT. Zij vragen of, als dat niet geval is, dat niet wenselijk is voor de interoperabiliteit tussen aanbieders en systemen.

Eenheid van taal en techniek is onderdeel van het Nederlandse beleid om tot interoperabiliteit en databeschikbaarheid te komen. Belangrijk aspect daarvan is het maken van afspraken omtrent te gebruiken standaarden, zoals SNOMED, LOINC en FHIR. In de EHDS-verordening worden er eisen gesteld voor de uitwisseling van gezondheidsgegevens. Bij de ontwikkeling van deze vereisten wordt gebruik gemaakt van bestaande internationale standaarden zoals SNOMED. Deze vereisten zullen uiteindelijk ook gelden voor EPD-systemen. Leveranciers dienen hun producten verplicht daarop aan te passen alvorens deze op de Europese markt worden aangeboden.

De leden van de fractie van JA21 geven aan graag toegelicht te zien wie de kosten draagt voor compliance aan EHDS-verordening.

De kosten voor compliance van EPD-systemen aan de vereisten uit de EHDS-verordening moeten door de leveranciers zelf worden gedragen.

Ten slotte vernemen zij graag hoe de naleving van de verschillende uitwisselingsregimes onder EHDS-verordening wordt geborgd.

De EHDS-verordening kent voor primair gebruik onder andere een regime voor het uitwisselen van persoonlijke elektronische gezondheidsgegevens tussen zorgaanbieders en -professionals onderling, ongeacht de lidstaat waar de zorgaanbieder is gevestigd. Voor de uitvoering en handhaving van de bepalingen in de context van primair gebruik moet Nederland een digitale gezondheidsautoriteit aanwijzen. Deze autoriteit houdt bijvoorbeeld toezicht op het nationale contactpunt voor primair gebruik en een burger of zorgprofessional kan bij deze autoriteit een klacht indienen bij vermoeden van niet naleving.

Verder kent de EHDS-verordening bij secundair gebruik een regime voor het beschikbaar maken van, en toegang verlenen tot, elektronische gezondheidsgegevens. Daarvoor moet Nederland een of meer instanties voor toegang tot gezondheidsgegevens (ook wel Health Data Access Bodies-HDAB) aanwijzen die verantwoordelijk is/zijn voor het verlenen van toegang tot elektronische gezondheidsgegevens in een beveiligde verwerkingsomgeving die het risico minimaliseert van onrechtmatige handelingen. De HDAB is verantwoordelijk voor het toezicht op het gebruik van gezondheidsgegevens binnen de beveiligde verwerkingsomgeving. Daarnaast is de HDAB ook verantwoordelijk voor het auditen van de beveiligde verwerkingsomgeving om ervoor te zorgen dat aan de hoogste normen van privacy en veiligheid wordt voldaan. Ook is de HDAB belast met de taak om niet naleving te sanctioneren.

Aanvullend is belangrijk op te merken dat er ook toezicht moet worden gehouden op de naleving van de EHDS-verordening-vereisten door leveranciers van EPD-systemen. Hiertoe dient een markttoezichthouder te worden aangewezen. Denkbaar is dat de Inspectie Gezondheidszorg en Jeugd (IGJ) hier een rol in kan gaan spelen aangezien deze toezichthoudende taak in grote mate overlap vertoont met de taken die zij zullen uitvoeren in het kader van de Wegiz.

Daarnaast moeten de eerder genoemde publieke organen nauw samenwerken met de Autoriteit Persoonsgegevens die verantwoordelijk blijft voor privacy-gerelateerde vraagstukken en de handhaving van de AVG.