Ministerie van Volksgezondheid,
Welzijn en Sport

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
4337644-1093673-DICIO

Bijlage(n)
1

Uw kenmerk
27529 nr 353

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 11 mei 2026
Betreft Verslag Schriftelijk Overleg (VSO) inzake SO Inbreng Informatieveiligheid in de zorg 27529 nr 353

Geachte voorzitter,

Hierbij bied ik u mijn reactie aan op de vragen die gesteld zijn in Verslag Schriftelijk Overleg (VSO) inzake SO Inbreng Informatieveiligheid in de zorg d.d. 21 januari 2026 (Kamerstuk 27529 nr 353).

Hoogachtend,

de minister van Langdurige Zorg,
Jeugd en Sport,

Mirjam Sterk

Inhoudsopgave **blz.**

I. Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met belangstelling kennisgenomen van de brief van de minister over de ontwikkelingen op het gebied van informatieveiligheid in de zorgsector. Deze leden onderschrijven het grote belang van een veilig en betrouwbaar gezondheidsinformatiestelsel als randvoorwaarde voor goede, toegankelijke en toekomstbestendige zorg.

De leden van de D66-fractie lezen in de brief dat het gebruik van clouddiensten in de zorgsector steeds verder toeneemt en dat hiermee ook de afhankelijkheid van specifieke leveranciers groeit. Deze leden vragen of de minister zicht heeft op de mate waarin de Nederlandse zorgsector afhankelijk is van specifieke clouddiensten en leveranciers, in het bijzonder waar het gaat om cruciale infrastructuur zoals ziekenhuizen en spoedzorg. Kan de minister aangeven in hoeverre zorginstellingen in staat zijn om bij verstoringen of uitval van deze diensten zelfstandig te blijven functioneren? Worden dergelijke scenario's structureel getest, bijvoorbeeld via continuïteitsplannen of crisisoefeningen, en welke lessen worden daaruit getrokken?

Deze leden begrijpen dat zorgaanbieders primair zelf verantwoordelijk zijn voor hun risicobeoordelingen en leverancierskeuzes. Tegelijkertijd vragen zij of de minister wil verkennen welke meer sturende en monitorende rollen voor het Rijk beschikbaar zijn om digitale afhankelijkheden in de zorg beter in beeld te brengen en te beheersen. Is de minister bereid te onderzoeken of sectorbrede monitoring van kritieke afhankelijkheden

wenselijk is, en of bijvoorbeeld minimumeisen kunnen worden gesteld aan exit-strategieën en continuïteitsvoorzieningen bij het gebruik van clouddiensten?

De leden van de D66-fractie lezen in de brief dat het incident bij Clinical Diagnostics voor de Inspectie Gezondheidszorg en Jeugd (IGJ) aanleiding is om laboratoria nadrukkelijker in het toezicht te betrekken en dat eventuele specifieke risico's die uit de lopende onderzoeken naar voren komen als aandachtspunt zullen worden meegenomen bij het toezicht in andere zorgsectoren. Deze leden benadrukken dat het hier gaat om een zeer ernstig incident waarbij gevoelige gegevens zijn buitgemaakt. Zij vragen de minister wat de huidige stand van zaken is van de onderzoeken naar dit incident en wanneer de Kamer hierover concreet zal worden geïnformeerd. Ook vragen zij hoe wordt geborgd dat eventuele structurele kwetsbaarheden die hieruit naar voren komen niet vrijblijvend worden opgevolgd, maar leiden tot duidelijke verbetermaatregelen.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met interesse kennisgenomen van de brief over de informatieveiligheid in de zorg. Ze hebben hierover enkele vragen.

In de brief die de minister op 4 december 2025 naar de Kamer heeft gestuurd, staan talloze bestuurlijke plannen omtrent dataveiligheid. De leden van de VVD-fractie onderschrijven het belang van dataveiligheid, maar erkennen ook de diversiteit en complexiteit ervan. Kan de minister reflecteren op het diverse en complexe beleid omtrent dataveiligheid? Acht hij de huidige "versnippering" gewenst?

De toegenomen veiligheidsdreiging moet volgens de leden van de VVD-fractie het hoofd worden geboden en zij zijn daarom verheugd te lezen dat de minister ambitieuze plannen heeft. Genoemde leden achten samenwerking essentieel in het realiseren van deze plannen. Zij hebben voorkeur in het bieden van vroegtijdige duidelijkheid richting zorgorganisaties over wat hen te wachten staat. Deze leden vragen of zorgorganisaties nog duidelijkheid ervaren over het huidige en toekomstige dataveiligheidsbeleid. De leden van de VVD-fractie vragen verder of er voor zorgorganisaties toegankelijke informatie beschikbaar is over het toekomstige beleid. Wordt toekomstig beleid verwerkt in de bestaande NEN normen?

De leden van de VVD-fractie lezen dat de IGJ een grote rol krijgt in het controleren van zorgorganisaties in het naleven van hun verplichtingen omtrent dataveiligheid. Deze leden lezen ook dat de IGJ hier meer middelen voor krijgt, maar vragen of de IGJ deze middelen ook toereikend acht. Kan de minister verduidelijken of hij overeenstemming had met de IGJ over de hoeveelheid extra financiële middelen?

De minister verwijst in de brief naar de invoering van de European Health Data Space-verordening (EHDS) bij het onderdeel "Bouwen aan een veilig gezondheidsinformatiestelsel". In hoeverre ligt de invoering hiervan op schema? Wat is de huidige verwachting van de invoeringsdatum? De leden van de VVD-fractie vragen dit in verband met de nog steeds nadrukkelijke wens die zij hebben, gesteund door vrijwel het hele zorgveld en patiëntenorganisaties, om te komen tot een opt-out voor

gegevensdeling voor de acute zorg en spoedeisende hulp. De minister heeft aangegeven hiermee te willen wachten tot de inwerkingtreding van de EHDS. Is de minister bereid, bij eventuele vertraging, de opt-out voor de acute zorg toch eerder mogelijk te maken? Genoemde leden merken daarbij overigens op dat zij nog steeds van mening zijn dat de opt-out voor de acute zorg op zo kort mogelijke termijn mogelijk moet zijn.

Bij het onderdeel “Inspelen op gewijzigd dreigingsbeeld en technologische ontwikkelingen” willen deze leden nog eens wijzen op de aangenomen motie Bushoff/Bevers “Bezien of bij fusies en overnames vanuit het buitenland van digitale zorginfrastructuur vergelijkbare voorwaarden gesteld kunnen worden als bij andere cruciale sectoren”, Kamerstuk 27 529, nr. 349. Kan de minister aangeven of hij het met de leden van de VVD-fractie de mening deelt dat het verzoek in de motie ook onderdeel is van de strategie ten aanzien de andere en grotere dreigingen die we wereldwijd zien op het gebied van dataveiligheid?

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de brief over het thema van informatieveiligheid in de zorg. Zij hebben hierbij nog enkele vragen.
De leden van de GroenLinks-PvdA-fractie lezen dat zorgaanbieders primair verantwoordelijk zijn voor hun informatiebeveiliging en dat de rol van de overheid vooral ondersteunend en stimulerend is. Zij maken zich echter zorgen, gelet op de nieuwsberichten en casuïstiek waarbij de informatieveiligheid niet op orde is. Acht de minister het houdbaar om informatiebeveiliging in de zorg hoofdzakelijk als een onderdeel van de bedrijfsvoering van individuele zorgaanbieders te blijven beschouwen, zeker gelet op het feit dat het falen van dergelijke systemen directe gevolgen heeft voor patiënten en eventueel de (continuïteit van) zorg? Kan nader worden toegelicht welke concrete rol u voor uzelf ziet weggelegd in het voorkomen en reageren op cyberaanvallen? Kan de minister tevens nader reflecteren op de balans tussen de marktwerking in zorg-ICT en de publieke regie op informatieveiligheid, mede in het licht van ketenafhankelijkheden?

De leden van de GroenLinks-PvdA-fractie lezen tevens dat er nog verschillende onderzoeken lopen naar de hack en het datalek bij Clinical Diagnostics en dat toegezegd wordt dat de Kamer doorlopend op de hoogte wordt gehouden over deze situatie en de maatregelen die zijn, en mogelijk nog, worden getroffen. Kan nader worden toegelicht welke maatregelen tot op heden zijn getroffen naar aanleiding van de hack?

De leden van de GroenLinks-PvdA-fractie lezen dat de naleving van de NEN 7510 norm (de Nederlandse norm voor informatiebeveiliging in de zorg) al jaren tekortschiet, ondanks wettelijke verplichtingen en toezicht door de IGJ. Kan nader toegelicht worden hoeveel zorgaanbieders op dit moment aantoonbaar wel voldoen aan NEN 7510, uitgesplitst naar sector en omvang? Hoe reflecteert de minister op het feit dat naleving pas na meerdere toezichtcycli en verbetertrajecten op niveau komt, terwijl er ondertussen reële risico’s bestaan voor patiënten?

De leden van de GroenLinks-PvdA-fractie lezen dat kleine zorgaanbieders vaker moeite hebben met de naleving van de normen en verplichtingen. Kan nader toegelicht worden hoe wordt voorkomen dat kleine zorgaanbieders onevenredig worden belast door de cumulatie van verplichtingen uit NEN normen, de Cyberbeveiligingswet (Cbw), de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) en de European Health Data

Space-verordening (EHDS)? Kan tevens nader toegelicht worden hoe zij hierin ondersteund zouden kunnen worden?

De leden van de GroenLinks-PvdA-fractie maken zich ten slotte ernstige zorgen over de grote afhankelijkheid van vaak niet-Europese cloud- en ICT-leveranciers in de zorg. Zij hechten veel waarde aan digitale autonomie, zeker in tijden van grote onzekerheid. Is de minister bereid om, in lijn met eerdere Kameruitspraken, het gebruik van Europese en open source-oplossingen actiever te stimuleren?

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben kennisgenomen van de brief van de minister over informatieveiligheid in de zorg en hebben hierover nog enkele vragen.

Wanneer ontvangt de Kamer verdere informatie over het onderzoek naar de hack bij het lab Clinical Diagnostics? Welke gevolgen heeft de Cyberbeveiligingswet (Cbw) voor het zorgveld?

De minister heeft voor naleving van de NEN 7510 norm voor kleinere zorginstellingen een quickscan beschikbaar gesteld. In hoeverre wordt daar gebruik van gemaakt? Hoe brengt de minister kleinere instellingen van het bestaan hiervan op de hoogte? Welke redenen geeft de IGJ voor ondermaatse naleving van de normen? Verschillende die per zorgveld?
De minister gaat een verkenning doen naar het centraal en uniform beschikbaar maken van hulpmiddelen voor informatiebeveiliging. Wanneer kan de Kamer hiervan resultaat verwachten?

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben kennisgenomen van de brief van de minister over informatieveiligheid in de zorg en hebben hierover nog enkele vragen.

Naar aanleiding van paragraaf 2.2.1 Cyberbeveiligingswet (Cbw). De leden van de CDA-fractie constateren dat de Cyberbeveiligingswet (Cbw) grote impact gaat hebben en veel zal vragen van organisaties, niet in het minst van zorgaanbieders. Deze leden vragen of de minister wil toelichten wat de gevolgen zijn van de Cyberbeveiligingswet voor zorgaanbieders en of er specifieke uitdagingen zijn in de implementatie voor zorgaanbieders. Zo ja, dan vragen deze leden hoe de minister deze punten adresseert. Genoemde leden zijn benieuwd naar de ministeriële regeling voor de zorg, en vragen wanneer deze naar verwachting naar de Kamer komt en welke elementen deze regeling bevat.

Naar aanleiding van paragraaf 2.4 Toezicht. De leden van de CDA-fractie lezen dat de IGJ constateert dat de naleving van NEN normen door zorgaanbieders achterblijft. Los van de acties van de minister om zorgaanbieders te ondersteunen vragen deze leden ook naar de rol van de IGJ. Zij vragen hoe de IGJ hiermee omgaat en of en zo ja, de IGJ extra inzet op handhaving of andere interventies. Ook vragen deze leden welke andere sectoren, naast de ziekenhuiszorg, gehandicaptenzorg en ouderenzorg aandacht krijgen van de IGJ.

Naar aanleiding van paragraaf 3.2.1 Digitale autonomie. De leden van de CDA-fractie maken zich zorgen over de snel opvolgende geopolitieke ontwikkelingen, die het belang van digitale autonomie alleen maar meer benadrukken. Zij vragen of de minister dit deelt en zo ja, of het dan voldoende is de sector op te roepen dit in hun afwegingen mee te nemen. Zoals de minister terecht aangeeft, is zorgverlening vaak kritieke dienstverlening die niet kan wachten. Deze leden vragen daarom wat de minister van VWS specifiek doet om bij zorg-IT-systemen digitaal autonomer te worden. Zij vragen of de minister nader wil toelichten waarom hij niet een meer dwingend kader aan de sector wil meegeven. Zij vragen wat de minister doet om in het cloudbeleid specifiek aandacht te besteden aan de zorgsector, vanwege het cruciale publieke belang.

De leden van de CDA-fractie vragen tot slot naar het advies van de Autoriteit Consument & Markt (ACM) over het verbeteren van de zorg-ICT-markt. Deze leden vragen of de minister deelt dat een betere ICT-markt, met minder afhankelijkheid van enkele leveranciers ook bijdraagt aan informatieveiligheid in de zorg. Deze leden vragen of de minister wil ingaan op de aanbevelingen van de ACM uit januari 2025.

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van de brief over informatieveiligheid in de zorg. Genoemde leden hebben geen vragen aan de minister.

II. Reactie van de minister

De leden van de D66-fractie hebben met belangstelling kennisgenomen van de brief van de minister over de ontwikkelingen op het gebied van informatieveiligheid in de zorgsector. Deze leden onderschrijven het grote belang van een veilig en betrouwbaar gezondheidsinformatiestelsel als randvoorwaarde voor goede, toegankelijke en toekomstbestendige zorg.

De leden van de D66-fractie lezen in de brief dat het gebruik van clouddiensten in de zorgsector steeds verder toeneemt en dat hiermee ook de afhankelijkheid van specifieke leveranciers groeit. Deze leden vragen of de minister zicht heeft op de mate waarin de Nederlandse zorgsector afhankelijk is van specifieke clouddiensten en leveranciers, in het bijzonder waar het gaat om cruciale infrastructuur zoals ziekenhuizen en spoedzorg. Kan de minister aangeven in hoeverre zorginstellingen in staat zijn om bij verstoringen of uitval van deze diensten zelfstandig te blijven functioneren? Worden dergelijke scenario's structureel getest, bijvoorbeeld via continuïteitsplannen of crisisoefeningen, en welke lessen worden daaruit getrokken?

Ik heb geen inzicht in de mate waarin de Nederlandse zorgsector afhankelijk is van leveranciers of specifieke clouddiensten. Een te grote eenzijdige afhankelijkheid kan risico's met zich brengen voor de continuïteit van zorg. Zorginstellingen zijn zelf verantwoordelijk de risico's in kaart te brengen. In de Kamerbrief over informatieveiligheid in de zorg van 4 december 2025 ben ik verder ingegaan op het

belang van digitale autonomie. Ik roep de sector daarom op om in hun risicoafwegingen de afhankelijkheid van leveranciers mee te nemen. Het doen van een risicoanalyse is onderdeel van de norm voor informatieveiligheid in de zorg (NEN7510). Aan deze norm dienen zorginstellingen aantoonbaar te voldoen. Bij het werken volgens de norm hoort ook het nemen van maatregelen om uitval (door bijvoorbeeld een cyberincident) te voorkomen en de impact te beperken. Een belangrijk onderdeel van de norm is bovendien dat er plannen worden gemaakt voor bedrijfscontinuïteit bij onverwachte verstoringen of uitval en dat deze periodiek getest, geëvalueerd en verbeterd worden.

Deze leden begrijpen dat zorgaanbieders primair zelf verantwoordelijk zijn voor hun risicobeoordelingen en leverancierskeuzes. Tegelijkertijd vragen zij of de minister wil verkennen welke meer sturende en monitorende rollen voor het Rijk beschikbaar zijn om digitale afhankelijkheden in de zorg beter in beeld te brengen en te beheersen. Is de minister bereid te onderzoeken of sectorbrede monitoring van kritieke afhankelijkheden wenselijk is, en of bijvoorbeeld minimumeisen kunnen worden gesteld aan exit-strategieën en continuïteitsvoorzieningen bij het gebruik van clouddiensten?

Ik deel uw zorgen voor wat betreft digitale afhankelijkheden in de zorg. Echter, het is en blijft de verantwoordelijkheid van de zorgaanbieder om hiervoor handelingsperspectieven op te stellen op basis van hun individuele risicoafwegingen. Uit de verantwoordelijkheid van de zorgaanbieder volgt dat zij zelf de afwegingen zullen maken, passend bij de eigen context. Er bestaat hiervoor namelijk geen '*quick fix*' of '*one size fits all*'.

Bijzondere aandacht in het kader van digitale autonomie verdient de risicoanalyse bij de inzet van cloud-toepassingen, omdat die vaak zorgt voor een grotere afhankelijkheid van leveranciers. De norm voor informatiebeveiliging in de zorg (NEN7510) bevat beheersmaatregelen voor het gebruik van clouddiensten. Waar overwogen wordt om cloud-toepassingen in te zetten of al ingezet zijn, adviseer ik om het Implementatiekader Risicoafweging Cloudgebruik[1] voor de Rijksoverheid te gebruiken. De Rijksoverheid is daarnaast bezig met een herziening van het Rijkscloudbeleid naar aanleiding van recente geopolitieke ontwikkelingen. Na vaststelling van dit nieuwe Rijkscloud beleid zal ik de gesprekken met Cumuluz, als uitvoeringsorganisatie van een landelijk dekkend netwerk, intensiveren om te komen tot een passende en proportionele vertaling van dit rijksbeleid naar de zorg. Uitvoering en implementatie zal daarna tijd kosten, maar het is eerst van belang nieuwe en heldere kaders te schetsen.

De leden van de D66-fractie lezen in de brief dat het incident bij Clinical Diagnostics voor de Inspectie Gezondheidszorg en Jeugd (IGJ) aanleiding is om laboratoria nadrukkelijker in het toezicht te betrekken en dat eventuele specifieke risico's die uit de lopende onderzoeken naar voren komen als aandachtspunt zullen worden meegenomen bij het toezicht in andere zorgsectoren. Deze leden benadrukken dat het hier gaat om een zeer ernstig incident waarbij gevoelige gegevens zijn buitgemaakt. Zij vragen de minister wat de huidige stand van zaken is van de onderzoeken naar dit incident en wanneer de Kamer hierover concreet zal worden geïnformeerd. Ook vragen zij hoe wordt geborgd dat eventuele structurele kwetsbaarheden die hieruit naar voren komen niet vrijblijvend worden opgevolgd, maar leiden tot duidelijke verbetermaatregelen.

[1] Implementatiekader risicoafweging cloudgebruik, versie 1.1, (CIO Rijk – Interdepartementale Commissie Bedrijfsvoering Rijksdienst), https://open.overheid.nl/documenten/ronl-734f947ec6465e4f75a56bed82fe64a1135f71a8/pdf (5 januari 2023)

De voormalig Staatsecretaris voor Jeugd, Preventie en Sport heeft in haar brief van 2 september 2025[2] aan uw Kamer laten weten dat er door verschillende partijen onderzoek wordt gedaan naar het datalek. Inmiddels heeft zij in haar brief van 5 februari 2026 laten weten dat er in opdracht van Bevolkingsonderzoek Nederland (BVO NL) onafhankelijk onderzoek is uitgevoerd naar de informatiebeveiliging binnen Clinical Diagnostics (CD)[3]. Het onderzoek bestond uit een analyse van het operationele proces, de IT-systemen, datastromen en onderliggende IT-infrastructuur van CD. Uit het onderzoeksrapport volgt dat op al die punten tekortkomingen bestaan. De samenwerking met CD is na bekendwording van de hack opgeschort en is dat tot op heden nog steeds. CD is nu op basis van het rapport aan de slag om de informatiebeveiliging op orde te brengen. BVO NL zal de samenwerking met CD alleen hervatten wanneer de veiligheid van de data van de deelnemers onafhankelijk is vastgesteld. Daarnaast heb ik vernomen dat Inspectie Gezondheidszorg en Jeugd (IGJ), de Autoriteit Persoonsgegevens (AP) en het Openbaar Ministerie (OM) ook onderzoek doen. Gezien hun onafhankelijke positie, is het mij niet bekend wanneer deze onderzoeken gereed zijn. Bij BVO NL is op basis van de recent afgeronde aanbesteding voor het bevolkingsonderzoek darmkanker sprake van voortschrijdend inzicht over de mogelijkheden rond verdere dataminimalisatie. Het risico op een omvangrijke hack bij contractpartijen was eerder geen onderdeel van het risicomanagementsysteem. BVO NL heeft dat nu wel als expliciet onderdeel opgenomen.

De leden van de VVD-fractie hebben met interesse kennisgenomen van de brief over de informatieveiligheid in de zorg. Ze hebben hierover enkele vragen.

In de brief die de minister op 4 december 2025 naar de Kamer heeft gestuurd, staan talloze bestuurlijke plannen omtrent dataveiligheid. De leden van de VVD-fractie onderschrijven het belang van dataveiligheid, maar erkennen ook de diversiteit en complexiteit ervan. Kan de minister reflecteren op het diverse en complexe beleid omtrent dataveiligheid? Acht hij de huidige "versnippering" gewenst?

Ik erken dat informatieveiligheid een complex en divers vraagstuk is. Daarom heb ik ervoor gezorgd het beleid omtrent dataveiligheid zo integraal mogelijk te houden en hanteren we een normenkader bedoeld voor de gehele zorgsector. In de Kamerbrief beschrijf ik de verschillende beleidsinstrumenten, zoals bijvoorbeeld het programma dat bewustwording stimuleert en het expertisecentrum Z-CERT dat ondersteunt bij incidenten. Op papier lijken dit strikt gescheiden onderwerpen en losstaande dossiers, maar in de praktijk zijn de initiatieven met elkaar verbonden. De samenwerking tussen (van overheidswege gesubsidieerde) instellingen is prima, vanuit verschillende expertises vult men elkaar aan. Ik doel dan op partners op het thema van informatieveiligheid in de zorg, zoals bijvoorbeeld Z-CERT, het Nederlands Normalisatie Instituut (NEN), ECP, de koepels- en brancheorganisaties en de inspectie gezondheid en Jeugd (IGJ). Vanuit één kader en ambitie treden zij het versnipperde zorgveld tegemoet.

De toegenomen veiligheidsdreiging moet volgens de leden van de VVD-fractie het hoofd worden geboden en zij zijn daarom verheugd te lezen dat de minister ambitieuze plannen heeft. Genoemde leden achten samenwerking essentieel in het realiseren van deze plannen. Zij hebben voorkeur in het bieden van vroegtijdige duidelijkheid richting zorgorganisaties over

[2] *Kamerstukken II*, 2024/25, 32761, nr. 330
[3] *Kamerstukken II*, 2025/26, 32 793, nr. 391

wat hen te wachten staat. Deze leden vragen of zorgorganisaties nog duidelijkheid ervaren over het huidige en toekomstige dataveiligheidsbeleid. De leden van de VVD-fractie vragen verder of er voor zorgorganisaties toegankelijke informatie beschikbaar is over het toekomstige beleid. Wordt toekomstig beleid verwerkt in de bestaande NEN normen?

Ik ben het met de leden eens dat verbinding met het veld en samenwerking belangrijk is voor het tegengaan van digitale dreigingen. Daarom organiseer ik elk kwartaal een overleg met koepels en branche organisaties. In deze overleggen presenteer en toets ik mijn toekomstige beleidsplannen. Ook haal ik informatie op binnen de deelsectoren van de zorg en worden ontwikkelingen en actualiteiten besproken. Daarnaast publiceer ik op de website 'data voor gezondheid' met grote regelmaat wat de (nieuwe) plannen zijn met betrekking tot het gezondheidsinformatiestelsel[4]. De plannen voor dataveiligheid zijn hier onderdeel van. Toekomstige ontwikkelingen en beleidsplannen worden tot slot meegenomen in de ontwikkeling van de NEN normen. Om de paar jaar wordt bijvoorbeeld de NEN7510 herzien. De meest recente herziening vond eind 2024 plaats.[5] Bij de ontwikkeling van een herziene NEN norm zijn vertegenwoordigers van alle belanghebbende partijen nauw betrokken. Als belanghebbende is VWS aangesloten bij de herzieningswerkgroep. Bij de herziening wordt gekeken naar de huidige ontwikkeling en stand van zaken, zoals actuele of nieuwe beleidsplannen van VWS.

De leden van de VVD-fractie lezen dat de IGJ een grote rol krijgt in het controleren van zorgorganisaties in het naleven van hun verplichtingen omtrent dataveiligheid. Deze leden lezen ook dat de IGJ hier meer middelen voor krijgt, maar vragen of de IGJ deze middelen ook toereikend acht. Kan de minister verduidelijken of hij overeenstemming had met de IGJ over de hoeveelheid extra financiële middelen?

De IGJ heeft al een rol in het toezicht op informatiebeveiliging op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). De IGJ krijgt ook een rol in het toezicht op (digitale) weerbaarheid op basis van de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke). Deze regelgeving bevindt zich in verschillende fasen van ontwikkeling en de rol van de IGJ is daar een afgeleide van. Daarbij blijven de uitdagingen rondom weerbaarheid zich steeds ontwikkelen.
Overigens ben ik permanent in gesprek met de IGJ over de balans tussen (nieuwe) taken en beschikbare middelen.

De minister verwijst in de brief naar de invoering van de European Health Data Space-verordening (EHDS) bij het onderdeel "Bouwen aan een veilig gezondheidsinformatiestelsel". In hoeverre ligt de invoering hiervan op schema? Wat is de huidige verwachting van de invoeringsdatum? De leden van de VVD-fractie vragen dit in verband met de nog steeds nadrukkelijke wens die zij hebben, gesteund door vrijwel het hele zorgveld en patiëntenorganisaties, om te komen tot een opt-out voor gegevensdeling voor de acute zorg en spoedeisende hulp. De minister heeft aangegeven hiermee te willen wachten tot de inwerkingtreding van de EHDS. Is de minister bereid, bij eventuele vertraging, de opt-out voor de acute zorg toch eerder mogelijk te maken? Genoemde leden merken daarbij overigens op dat zij nog steeds van mening zijn dat de opt-out voor de acute zorg op zo kort mogelijke termijn mogelijk moet zijn.

[4] Data voor gezondheid | Data voor gezondheid
[5] https://www.nen.nl/nieuws/actueel/herziene-nen-7510-gepubliceerd-/

Net als de leden van de VVD-fractie, vind ik het ook heel belangrijk dat er een opt-out komt. Er wordt dan ook hard gewerkt aan het mogelijk maken van een opt-out, waarbij gegevens breed kunnen worden uitgewisseld, maar waarbij burgers ook kunnen aangeven wanneer zij niet willen dat hun gegevens worden gedeeld.

Voor een opt-out in de acute zorg is eerder gewerkt aan een nationaal wetsvoorstel (Wogaz). In februari 2025 is de EHDS-verordening in werking getreden. De EHDS heeft qua reikwijdte grote overlap met de Wogaz. De EHDS biedt de mogelijkheid om een opt-out-recht wettelijk in te regelen voor alle zorgsectoren die onder de reikwijdte van de EHDS vallen, waaronder de acute zorg. Om te voorkomen dat er twee wetstrajecten met hetzelfde doel gelijktijdig worden ontwikkeld, en mogelijk door elkaar heen gaan lopen, wordt alle aandacht gericht op de realisatie van de EHDS. Dit is ook met uw Kamer besproken in het commissiedebat van 10 april 2025 en het tweeminutendebat van 4 september jl. De opt-out voor de acute zorg (en alle andere zorgsectoren die onder de reikwijdte van de EHDS vallen) zal dus gelijktijdig met de Nederlandse EHDS-implementatiewetgeving tot stand komen. Ik ben voornemens om de deadline, namelijk maart 2029, hiervoor aan te houden. Op dit moment wordt gewerkt aan de vormgeving van de opt-out. Zoals mijn voorganger in de Kamerbrief van januari 2026[6] heb toegezegd, zal ik de Tweede Kamer na de zomer 2026 informeren over het gehele burgerrechtenstelsel van de EHDS, inclusief de opt-out. Ik werk daarnaast – samen met de gehele spoedzorgketen – hard aan het realiseren van snelle en veilige gegevensuitwisseling in de acute zorg door middel van het programma Met Spoed Beschikbaar.

Bij het onderdeel "Inspelen op gewijzigd dreigingsbeeld en technologische ontwikkelingen" willen deze leden nog eens wijzen op de aangenomen motie Bushoff/Bevers "Bezien of bij fusies en overnames vanuit het buitenland van digitale zorginfrastructuur vergelijkbare voorwaarden gesteld kunnen worden als bij andere cruciale sectoren", Kamerstuk 27 529, nr. 349. Kan de minister
aangeven of hij het met de leden van de VVD-fractie de mening deelt dat het verzoek in de motie ook onderdeel is van de strategie ten aanzien de andere en grotere dreigingen die we wereldwijd zien op het gebied van dataveiligheid?

Zoals eerder in de Kamerbrief is toegelicht nemen digitale dreigingen in de zorg wereldwijd toe. Daarom werk ik binnen Europa gezamenlijk aan het versterken van de digitale weerbaarheid in de vitale sectoren, waaronder de gezondheidszorg. Ik werk samen met de minister van Justitie en Veiligheid (JenV) aan de implementatie van de Europese NIS2 richtlijn in de Cyberbeveiligingswet. Daarnaast wordt door minister van JenV en de minister van Economische Zaken nagegaan of de herziening van de Wet veiligheidstoets investeringen, fusies en overnames (Vifo) mogelijk gewijzigd moeten worden om te zorgen dat het aansluit op de stelselwijziging m.b.t. vitale aanbieders en processen door het invoeren van de Wet weerbaarheid kritieke entiteiten (Wwke).

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de brief over het thema van informatieveiligheid in de zorg. Zij hebben hierbij nog enkele vragen.

De leden van de GroenLinks-PvdA-fractie lezen dat zorgaanbieders primair verantwoordelijk zijn voor hun informatiebeveiliging en dat de rol van de overheid vooral ondersteunend en stimulerend is. Zij maken zich echter zorgen, gelet op de nieuwsberichten en casuïstiek

[6] *Kamerstukken II*, 2025/26, 529, nr. 356

waarbij de informatieveiligheid niet op orde is. Acht de minister het houdbaar om informatiebeveiliging in de zorg hoofdzakelijk als een onderdeel van de bedrijfsvoering van individuele zorgaanbieders te blijven beschouwen, zeker gelet op het feit dat het falen van dergelijke systemen directe gevolgen heeft voor patiënten en eventueel de (continuïteit van) zorg?

Ik herken uw zorgen, het is van groot belang de informatieveiligheid van de zorg te versterken om continuïteit van zorg te borgen. Het is en blijft zo dat zorginstellingen hiervoor in de eerste plaats zelf verantwoordelijk zijn. Dit doen zij door het werken volgens de normen voor informatieveiligheid. Toezicht op individuele zorginstellingen wordt steekproefsgewijs en risicogestuurd uitgevoerd door de Inspectie Gezondheid en Jeugd. Het werken volgens de normen is inherent onderdeel van de bedrijfsvoering en zou net zo vanzelfsprekend moeten zijn als andere onderdelen, zoals veiligheid van het gebouw en personeel. ICT-uitgaven of investeringen zouden dit belang moeten reflecteren. Ik heb hierin uitsluitend een stelselverantwoordelijke rol en ondersteun het veld met hulpmiddelen om de digitale weerbaarheid te versterken. De rol van de zorgbestuurder is in deze cruciaal aangezien de bestuurder binnen de organisatie de prioriteiten stelt. Lang niet altijd heeft dataveiligheid de aandacht van zorgbestuurders gehad, die het verdient. Dat moet anders, juist vanwege de potentiële impact op burgers en de continuïteit van zorg. Niet voor niets worden in de Cyberbeveiligingswet voor die instellingen die er onder gaan vallen harde eisen gesteld aan bestuurders.

Kan nader worden toegelicht welke concrete rol u voor uzelf ziet weggelegd in het voorkomen en reageren op cyberaanvallen?

In het voorkomen van cyberincidenten en het versterken van de informatieveiligheid neem ik een kaderstellende, toezichthoudende, stimulerende en faciliterende rol. Ik ondersteun zorginstellingen bij het voorkomen van incidenten door het verhogen van bewustzijn van zorgmedewerkers in het programma Informatieveilig gedrag in de zorg. Een groot deel van cyberincidenten zijn mede veroorzaakt door menselijk handelen. Daarnaast bied ik hulpmiddelen aan om te voldoen aan de NEN7510, de norm voor informatiebeveiliging in de zorg. Deze norm schrijft organisatorische, mensgerichte, fysieke en technologische beheersmaatregelen voor die de digitale weerbaarheid van een organisatie concreet verhogen. Dit met het doel om dreigingen te voorkomen, detecteren of erop te reageren. Tot slot helpt het expertisecentrum cybersecurity in de zorg (Z-CERT) zorginstellingen in het voorkomen van incidenten door te monitoren en eventuele dreigingsinformatie te delen. Daarnaast biedt Z-CERT ondersteuning bij het beperken van de gevolgen wanneer er onverhoopt een incident heeft plaatsgevonden.

Kan de minister tevens nader reflecteren op de balans tussen de marktwerking in zorg-ICT en de publieke regie op informatieveiligheid, mede in het licht van ketenafhankelijkheden?

Zorgaanbieders zijn verantwoordelijk voor de afspraken die gemaakt worden met hun ICT-leveranciers en daarmee voor het voldoen aan de NEN7510. In de NEN7510, de nationale wettelijke norm voor informatiebeveiliging in de zorg, staat dat het verplicht is een risicobeoordeling uit te voeren en digitale afhankelijkheden in kaart brengen is daar een onderdeel van. Daarnaast verplicht de Cyberbeveiligingswet (Cbw) organisaties om hun leveranciersketen in kaart te brengen, en om aan de leveranciers in die keten informatiebeveiligingsnormen te stellen. Ik ben me echter bewust dat (onder andere de kleinere) zorgaanbieders soms worstelen om het voldoen aan de NEN7510 af te dwingen

bij leveranciers. Zowel de koepels als in sommige gevallen de verzekeraars helpen met het organiseren van vraag articulatie en daarmee inkoopmacht.

De leden van de GroenLinks-PvdA-fractie lezen tevens dat er nog verschillende onderzoeken lopen naar de hack en het datalek bij Clinical Diagnostics en dat toegezegd wordt dat de Kamer doorlopend op de hoogte wordt gehouden over deze situatie en de maatregelen die zijn, en mogelijk nog, worden getroffen. Kan nader worden toegelicht welke maatregelen tot op heden zijn getroffen naar aanleiding van de hack?

In de brief van 5 februari 2026 heeft de voormalig Staatssecretaris van Jeugd, Preventie en Sport u geïnformeerd over de resultaten van het onderzoek dat in opdracht van Bevolkingsonderzoek Nederland (BVO NL) is uitgevoerd[7]. Daarnaast heb ik vernomen dat Inspectie Gezondheidszorg en Jeugd (IGJ), de Autoriteit Persoonsgegevens (AP) en het Openbaar Ministerie (OM) ook onderzoek doen. Gezien hun onafhankelijke positie, is het mij niet bekend wanneer deze onderzoeken gereed zijn. De samenwerking met Clinical Diagnostics (CD) is na bekendwording van de hack opgeschort en is dat tot op heden nog steeds. CD is nu op basis van het rapport aan de slag om de informatiebeveiliging op orde te brengen. BVO NL zal de samenwerking met CD alleen hervatten wanneer de veiligheid van de data van de deelnemers onafhankelijk is vastgesteld. Bij BVO NL is op basis van de recent afgeronde aanbesteding voor het bevolkingsonderzoek darmkanker is sprake van voortschrijdend inzicht over de mogelijkheden rond verdere dataminimalisatie. Het risico op een omvangrijke hack bij contractpartijen was eerder geen onderdeel van het risicomanagementsysteem. BVO NL heeft dat nu wel als expliciet onderdeel opgenomen.

De leden van de GroenLinks-PvdA-fractie lezen dat de naleving van de NEN 7510 norm (de Nederlandse norm voor informatiebeveiliging in de zorg) al jaren tekortschiet, ondanks wettelijke verplichtingen en toezicht door de IGJ. Kan nader toegelicht worden hoeveel zorgaanbieders op dit moment aantoonbaar wel voldoen aan NEN 7510, uitgesplitst naar sector en omvang? Hoe reflecteert de
minister op het feit dat naleving pas na meerdere toezichtcycli en verbetertrajecten op niveau komt, terwijl er ondertussen reële risico's bestaan voor patiënten?

Nederland kent een zeer groot aantal zorgaanbieders en de IGJ houdt daarom noodzakelijkerwijs risicogestuurd en steekproefsgewijs toezicht op dit informatieveiligheid. De IGJ heeft geen volledig en betrouwbaar kwantitatief beeld van hoeveel zorgaanbieders aantoonbaar wél voldoen aan NEN 7510 (en kan dit door het grote aantal zorgaanbieders ook niet hebben). Van sommige (kleinere) deelsectoren is er wel een meer betrouwbaar beeld, hetzij omdat alle aanbieders in deze sector zijn geïnspecteerd, dan wel aantoonbaar beschikken over een certificaat in het NEN-register. Zo voldoet het overgrote deel van de ziekenhuizen inmiddels aantoonbaar aan de norm[8] en is ook de naleving in de ambulancesector zeer hoog. In diverse andere sectoren heeft de IGJ de aandacht voor informatiebeveiliging de afgelopen jaren geïntensiveerd.

Ik ben me bewust van de risico's die gemoeid gaan met het niet voldoen aan de normen. De van toepassing zijnde NEN-normen verplichten zorginstellingen om deze risico's in kaart te brengen en om passende maatregelen te nemen. Het voldoen aan de norm is

[7] *Kamerstukken II*, 2025/26, 32 793, nr. 391

[8] Ziekenhuizen maken stevige inhaalslag met informatiebeveiliging | Inspectie Gezondheidszorg en Jeugd

een complexe taak met een diverse hoeveelheid aan onderdelen. Dit kan niet in een korte tijd bewerkstelligd worden. Door middel van informele interventies probeert de IGJ te bereiken dat zorgaanbieders zelf actie ondernemen. Dit is in lijn met de primaire verantwoordelijkheid die bij het veld ligt. Hoewel het tijd kost, zien we dat de cyclische aanpak van de IGJ werkt en dat verschillende sectoren verbeterde resultaten hebben laten zien. Ook is het belangrijk te benadrukken dat het duurzamer is om zorgaanbieders zelf met verbeterplannen in actie te laten komen; dataveiligheid is immers nooit 'af', het op gang brengen van een permanente verbetercyclus leidt op langere termijn tot een hoger niveau van dataveiligheid.

De leden van de GroenLinks-PvdA-fractie lezen dat kleine zorgaanbieders vaker moeite hebben met de naleving van de normen en verplichtingen. Kan nader toegelicht worden hoe wordt voorkomen dat kleine zorgaanbieders onevenredig worden belast door de cumulatie van verplichtingen uit NEN normen, de Cyberbeveiligingswet (Cbw), de Wet elektronische gegevensuitwisseling in de zorg (Wegiz) en de European Health Data Space-verordening (EHDS)? Kan tevens nader toegelicht worden hoe zij hierin ondersteund zouden kunnen worden?

De genoemde kaders of wetgevingstrajecten zijn gezamenlijk belangrijke voorwaarden om te komen tot een goed functionerend en integraal georganiseerd gezondheidsinformatiestelsel. Ze zijn en worden zo vormgegeven dat zij op elkaar aansluiten en elkaar versterken. Dit volgt onder meer uit de Nationale Visie en Strategie voor het Gezondheidsinformatiestelsel (NVS), waarin het creëren van samenhang een van de centrale doelen is. Die samenhang komt concreet tot uitdrukking in de genoemde kaders en wetstrajecten. Hieronder noem ik enkele voorbeelden.

Zo is er ten eerste verband tussen de NEN7510 en de Cyberbeveiligingswet (Cbw). Daarbij teken ik aan dat de Cbw niet voor alle zorgaanbieders van toepassing is. De Cbw is uitsluitend van toepassing wanneer een FTE-eis of een omzet eis wordt gehaald.[9] Door te voldoen aan de eisen in de NEN7510 wordt voldaan aan een groot deel van de eisen die voortkomen uit de zorgplicht van de Cbw. Ik onderneem verschillende acties om kleine zorgaanbieders daarbij te ondersteunen. Ik bied hulpmiddelen aan om te voldoen aan de NEN7510, onder andere voor bijvoorbeeld kleinere organisaties die de NEN7510 voor het eerst implementeren. Ik stel daarnaast voor kleinere zorgaanbieders een instrument beschikbaar om te bepalen welke maatregelen (nog) genomen moeten worden voor informatieveiligheid. Tot slot verstrek ik middelen aan het programma informatie veilig gedrag in de zorg. De zorgorganisaties die aan de slag gaan binnen het programma Informatieveilig gedrag geven hiermee een concrete invulling aan verschillende paragrafen uit de NEN7510.

Ten tweede stuur ik bij de implementatie van de European Health Data Space (EHDS) op een zo goede mogelijke aansluiting hierop van bestaande nationale wetgeving, zoals de Wegiz. Waar Nederland al werkte aan het verbeteren van elektronische gegevensuitwisseling en de kaders daarvoor onder de Wegiz, is op Europees niveau de EHDS ontwikkeld, die een wettelijk kader biedt voor databeschikbaarheid in de zorg. Nederland heeft actief bijgedragen om deze kaders zoveel mogelijk op elkaar te laten aansluiten. VWS hanteert daarom bij de verdere uitwerking van beleid, regelgeving en de meerjarenagenda de geprioriteerde categorieën van de EHDS als basis, aangevuld

[9] Cyberbeveiligingswet (Cbw) | Data voor gezondheid

met nationale doelen die hiermee in lijn zijn en relevant zijn voor de Nederlandse zorgpraktijk.

Kleine zorgaanbieders worden tot slot op meerdere manieren ondersteund binnen de implementatieprogramma's voor geprioriteerde gegevensuitwisselingen onder de WEGIZ. Een voorbeeld daarvan is het implementatieprogramma eOverdracht. Naast het onderdeel Kickstart IB&P[10] is binnen het programma eOverdracht expliciet aandacht voor hun specifieke behoeften. Zo is er in overleg met het zorgveld voor gekozen om de scope van de Algemene Maatregel van Bestuur (AMvB) eOverdracht in eerste instantie te laten gelden voor zorgaanbieders van 11 of meer FTE binnen de VVT, MSZ en GHZ. Kleinere zorgaanbieders krijgen vervolgens langer de tijd om te voldoen aan de AMvB eOverdracht. Tevens wordt met ECD-leveranciers gekeken wat er aanvullend benodigd is voor kleine zorgaanbieders. Kleine zorgaanbieders kunnen reeds ondersteund worden met het implementeren van de eOverdracht. De aanpak van het programma waarbij zorgaanbieders in natura middels een pool van projectleiders, en dus kennis en capaciteit worden ondersteund, is ook voor kleine zorgaanbieders zeer passend. Tenslotte is VWS in gesprek met BVKZ en ZorgthuisNL om te onderzoeken of er aanvullend nog meer nodig is voor kleine zorgaanbieders.

De leden van de GroenLinks-PvdA-fractie maken zich ten slotte ernstige zorgen over de grote afhankelijkheid van vaak niet-Europese cloud- en ICT-leveranciers in de zorg. Zij hechten veel waarde aan digitale autonomie, zeker in tijden van grote onzekerheid. Is de minister bereid om, in lijn met eerdere Kameruitspraken, het gebruik van Europese en open source-oplossingen actiever te stimuleren?

Ik deel deze zorgen, de huidige geopolitieke situatie maakt het noodzakelijk om voor kritieke maatschappelijke functies, zoals de zorg sector, autonomie vraagstukken in de risicoafwegingen nadrukkelijk mee te nemen. In de brief van mijn voorganger aan uw Kamer van 4 december 2025 is de sector dan ook opgeroepen om in hun risicoafwegingen de afhankelijkheid van leveranciers mee te nemen. Voor de inzet van specifieke technologie kan en wil ik geen dwingend kader aan de sector voorschrijven. Aangezien de zorgaanbieder in de eerste plaats zelf verantwoordelijk is voor zijn informatieveiligheid, zal die ook zelf de afwegingen moeten maken, passend bij de eigen context. Er bestaat hier geen '*quick fix*' of '*one size fits all*'. VWS ziet natuurlijk wel in welke invloed zij heeft op de sector en daarmee als goed voorbeeld kan dienen. Zo heeft de toenmalige minister van VWS uw Kamer eerder in de kamerbrieven van 30 maart 2025[11] en 12 maart 2025[12] geïnformeerd dat bij delen van het Gezondheid informatie stelsel een hoge mate van opensourcewerken wordt toegepast. Voor het GIS geldt dat deze als digitale publieke infrastructuur volgens een hoge mate van opensourcewerken zal worden ontwikkeld. De Rijksoverheid is daarnaast bezig met een herziening van het Rijkscloudbeleid naar aanleiding van recente geopolitieke ontwikkelingen. Na vaststelling van dit nieuwe Rijkscloud beleid zal ik de gesprekken met Cumuluz, als uitvoeringsorganisatie van een landelijk dekkend netwerk, intensiveren om te komen tot een passende en proportionele vertaling van dit rijksbeleid naar de zorg. Uitvoering en implementatie zal daarna tijd kosten, maar het is eerst van belang nieuwe en heldere kaders te schetsen.

[10] Kickstart IB&P voor organisaties in de langdurige zorg - Samen werken aan eOverdracht

[11] *Kamerstukken II*, 2024.25, 27 529, nr. 325

[12] *Kamerstukken II*, 2024.25, 27 529, nr. 331

De leden van de PVV-fractie hebben kennisgenomen van de brief van de minister over informatieveiligheid in de zorg en hebben hierover nog enkele vragen.

Wanneer ontvangt de Kamer verdere informatie over het onderzoek naar de hack bij het lab Clinical Diagnostics?

In de brief van 5 februari 2026 heeft de voormalig Staatssecretaris van Jeugd, Preventie en Sport u geïnformeerd over de resultaten van het onderzoek dat in opdracht van Bevolkingsonderzoek Nederland (BVO NL) is uitgevoerd[13]. Daarnaast heb ik vernomen dat Inspectie Gezondheidszorg en Jeugd (IGJ), de Autoriteit Persoonsgegevens (AP) en het Openbaar Ministerie (OM) ook onderzoek doen. Gezien hun onafhankelijke positie, is het mij niet bekend wanneer deze onderzoeken gereed zijn.

Welke gevolgen heeft de Cyberbeveiligingswet (Cbw) voor het zorgveld?

De Cyberbeveiligingswet verplicht organisaties die essentiële of maatschappelijk belangrijke diensten leveren — waaronder veel organisaties uit de zorgsector — om hun digitale weerbaarheid aantoonbaar op orde te hebben. Dit betekent het aantoonbaar beveiligen van netwerk- en informatiesystemen, het beheersen van cyberrisico's en het voorbereid zijn op digitale incidenten en het melden van significante cyberincidenten. Organisaties die onder de Cbw vallen zijn verplicht melding te maken van significante incidenten in het portaal van het Nationaal Cybersecurity Centrum (NCSC). Het Cyber Security Incident Response Team voor de zorg (Z-CERT) en de Inspectie Gezondheid en Jeugd zijn ook aangesloten op dit portaal.

De minister heeft voor naleving van de NEN 7510 norm voor kleinere zorginstellingen een quickscan beschikbaar gesteld. In hoeverre wordt daar gebruik van gemaakt? Hoe brengt de minister kleinere instellingen van het bestaan hiervan op de hoogte?

Vanaf medio december 2024 is de Quickscan informatiebeveiliging beschikbaar als onderdeel van de Kickstart Informatiebeveiliging en Privacy (Kickstart IB&P). De Kickstart IB&P is onderdeel van het implementatieprogramma eOverdracht en bedoeld om met name zorgorganisaties binnen de langdurige zorg te ondersteunen. Het is een middel die zorgorganisaties zelfstandig of met ondersteuning van een team van experts kunnen invullen. De uitkomsten geven snel inzage in de status van elf belangrijke elementen uit de NEN7510 norm. De quickscan is bij uitstek geschikt voor kleine zorgorganisaties (tot 100 fte) en kan
zelfstandig door hen worden doorlopen of onder begeleiding van het Kickstart-team. In de periode van 1 januari 2025 tot 1 februari 2026 is de quickscan 189 keer gedownload. In het geval zorgorganisaties ervoor kiezen om de quickscan onder begeleiding te doorlopen, worden de vervolgacties direct gezamenlijk geformuleerd en opgepakt onder begeleiding van het Kickstart IB&P-team. Uit de praktijk blijkt dat juist kleine zorgorganisaties behoefte hebben aan deze vorm van volledige ondersteuning tijdens een traject om hun informatiebeveiliging te verhogen.

Er wordt op verschillende manieren gewerkt aan het onder de aandacht brengen van de methode bij (kleine) zorgaanbieders. Kickstart IB&P is bijvoorbeeld ontwikkeld in afstemming met verschillende zorgorganisaties, partners als NEN en Z-CERT, brancheverenigingen als ActiZ, ZorgthuisNL, BVKZ en VGN. Via de websites en

[13] *Kamerstukken II*, 2025/26, 32 793, nr. 391

nieuwsbrieven van deze partijen wordt de Kickstart onder de aandacht gebracht bij hun leden of deelnemers. Ook wordt het bereik vergroot via LinkedIn en deelname aan vakbeurzen zoals de Zorg & ICT beurs en het Mobile Healthcare Festival. Tevens is het team betrokken bij het analyse- en vervolgtraject van de Inspectie Gezondheidszorg en Jeugd (IGJ) op hun rapport van juli 2025 inzake toezicht op de informatiebeveiliging van kleinere zorgaanbieders. Ook verzorgt het Kickstart-team in samenwerking met thuiszorg bracheorganisatie ZorgthuisNL webinars speciaal gericht op kleine zorgorganisaties. Daarnaast promoten de NEN-community en Digital Trust Center (DTC) het programma actief en zoekt het team voortdurend aansluiting bij regionale samenwerkingsorganisaties zoals regionale samenwerkingsorganisatie (RSO) Trijn en RSO Gelderse Vallei.

Welke redenen geeft de IGJ voor ondermaatse naleving van de normen? Verschillende die per zorgveld?

Er kunnen diverse redenen zijn waarom zorgaanbieders nog verbeteringen moeten doorvoeren om volledig en aantoonbaar aan de gestelde normen te voldoen. Verbeterpunten die de IGJ in haar toezicht tegenkomt zijn onder andere: meer bekendheid met de wettelijke verplichtingen, meer deskundigheid op het gebied van informatiebeveiliging, meer gevoel van urgentie bij het bestuur, voldoende beschikbare middelen, voldoende interne monitoring (bv. ontbreken van audits) en meer inzicht in de risico's van onvoldoende informatiebeveiliging. De IGJ kan niet kwantitatief aangeven in welke verhouding deze verbeterpunten zich voordoen per zorgveld.

De minister gaat een verkenning doen naar het centraal en uniform beschikbaar maken van hulpmiddelen voor informatiebeveiliging. Wanneer kan de Kamer hiervan resultaat verwachten?

Ik ga hier het komende jaar mee aan de slag en hiervoor kom ik uiterlijk in het derde kwartaal van 2026 met een strategie.

De leden van de CDA-fractie hebben kennisgenomen van de brief van de minister over informatieveiligheid in de zorg en hebben hierover nog enkele vragen.

Naar aanleiding van paragraaf 2.2.1 Cyberbeveiligingswet (Cbw). De leden van de CDA-fractie constateren dat de Cyberbeveiligingswet (Cbw) grote impact gaat hebben en veel zal vragen van organisaties, niet in het minst van zorgaanbieders. Deze leden vragen of de minister wil toelichten wat de gevolgen zijn van de Cyberbeveiligingswet voor zorgaanbieders en of er specifieke uitdagingen zijn in de implementatie voor zorgaanbieders. Zo ja, dan vragen deze leden hoe de
minister deze punten adresseert. Genoemde leden zijn benieuwd naar de ministeriële regeling voor de zorg, en vragen wanneer deze naar verwachting naar de Kamer komt en welke elementen deze regeling bevat.

De Cyberbeveiligingswet verplicht zorgaanbieders hun digitale weerbaarheid aantoonbaar te verhogen, met een zorgplicht en een meldplicht voor significante cyberincidenten. De zorgplicht houdt in dat organisaties die vallen onder de Cbw hun informatiebeveiliging verplicht op orde moeten hebben en zelf een risicobeoordeling uit te voeren. Op basis hiervan dienen zij passende maatregelen te nemen om digitale risico's te beperken en incidenten te voorkomen. De Cyberbeveiligingswet stelt dat een Cyber Security Incident Response Team (CSIRT) ondersteuning verleent voorafgaand en

tijdens een incident aan de organisaties waarop de wet van toepassing is. Het expertisecentrum cybersecurity in de zorg, Z-CERT, is het CSIRT voor de entiteiten in de zorg en de wettelijke taken van Z-CERT worden vastgelegd in de ministeriele regeling voor de sector zorg .

De organisaties die onder de Cbw vallen zijn ervoor verantwoordelijk dat hun rechtstreekse toeleveranciers de cyberbeveiliging op orde hebben. De organisatie kan aan de toeleveranciers verzoeken om mitigerende maatregelen te nemen om de bestaande cyber risico's te beheersen. Voor zorgaanbieders liggen specifieke uitdagingen in het borgen van voldoende capaciteit en expertise op het gebied van cyberbeveiliging, het inrichten van goed werkende incident- en meldprocessen en het meenemen van toeleveranciers en ICT-dienstverleners in de keten.

In de uitwerking van de ministeriële regeling voor het zorgveld worden de sectorspecifieke vereisten nader ingevuld. Er wordt ten eerste aangesloten bij de NEN7510 (norm voor informatiebeveiliging in de zorg) om aantoonbaar aan de zorgplicht te voldoen. Daarnaast worden er sectorspecifieke drempelwaarden uitgewerkt voor het melden van significante incidenten en wordt verduidelijkt welke categorieën zorgaanbieders onder de wet vallen. De Cyberbeveiligingswet en daarmee ook de ministeriele regeling voor de sector zorg zal, afhankelijk van parlementaire besluitvorming, in het tweede kwartaal van 2026 inwerking treden.

Naar aanleiding van paragraaf 2.4 Toezicht. De leden van de CDA-fractie lezen dat de IGJ constateert dat de naleving van NEN normen door zorgaanbieders achterblijft. Los van de acties van de minister om zorgaanbieders te ondersteunen vragen deze leden ook naar de rol van de IGJ. Zij vragen hoe de IGJ hiermee omgaat en of en zo ja, de IGJ extra inzet op handhaving of andere interventies. Ook vragen deze leden welke andere sectoren, naast de ziekenhuiszorg, gehandicaptenzorg en ouderenzorg aandacht krijgen van de IGJ.

De IGJ houdt risicogestuurd en steekproefsgewijs toezicht op informatiebeveiliging binnen de gehele sector gezondheidszorg. Daarnaast kunnen meldingen een aanleiding vormen om onderzoek te doen. In de afgelopen jaren is het toezicht op informatiebeveiliging geïntensiveerd en heeft de IGJ hierover diverse rapportages gepubliceerd[14]. De afgelopen periode heeft de IGJ specifieke doelgroepen uitgelicht, waaronder de ziekenhuiszorg, zelfstandige klinieken, huisartsendienstenstructuren, gehandicaptenzorg en ouderenzorg. Maar ook in andere sectoren als de eerstelijnszorg, geestelijke gezondheidzorg en jeugdhulpaanbieders houdt de IGJ toezicht op informatiebeveiliging. De IGJ houdt toezicht op informatiebeveiliging door middel van

[14] Professionele digitale zorg vraagt van ziekenhuizen steeds opnieuw evalueren en verbeteren, Inspectie Gezondheidszorg en Jeugd (IGJ), https://www.igj.nl/site/binaries/sitecontent/collections/documents/2021/12/21/professionele-digitale-zorg-vraagt-vanziekenhuizen-steeds-opnieuw-evalueren-en-verbeteren/73298_IGJ_Factsheet_TG.pdf (21december 2021)
Gehandicaptenzorg worstelt met digitale vormen van zorg, Inspectie Gezondheidszorg en Jeugd (IGJ), https://www.igj.nl/site/binaries/sitecontent/collections/documents/2023/06/16/publicatie-gehandicaptenzorg-worstelt-metdigitale-vormen vanzorg/Gehandicaptenzorg+worstelt+met+digitale+vormen+van+zorg.pdf (16 juni 2023)
Zeer grote zorgaanbieders ouderenzorg hebben digitale zorg op orde, informatiebeveiliging moet beter (IGJ), Zeer grote zorgaanbieders ouderenzorg hebben digitale zorg op orde, informatiebeveiliging moet beter | Inspectie Gezondheidszorg en Jeugd (IGJ), https://www.igj.nl/documenten/2025/06/05/digitale-zorg-bij-zeer-grote-zorgaanbieders (5 juni 2025)

het afleggen van inspectiebezoeken bij zorgaanbieders of door middel van het uitsturen van vragenlijsten gericht op informatiebeveiliging en de mate waarin naleving van de norm kan worden aangetoond. De IGJ blijft daarbij steeds kijken welke andere of aanvullende interventies per sector nodig zijn. Dit vindt ook plaats op basis van overleg met koepelorganisaties. Daar waar de IGJ constateert dat een zorgaanbieder niet aantoonbaar voldoet aan de NEN 7510, vraagt de IGJ om verbeterplannen en de uitvoering daarvan. De IGJ volgt de verbeterplannen bij zorgaanbieders totdat deze aanbieders kunnen aantonen te werken volgens de norm NEN 7510.

Naar aanleiding van paragraaf 3.2.1 Digitale autonomie. De leden van de CDA-fractie maken zich zorgen over de snel opvolgende geopolitieke ontwikkelingen, die het belang van digitale autonomie alleen maar meer benadrukken.

Zij vragen of de minister dit deelt en zo ja, of het dan voldoende is de sector op te roepen dit in hun afwegingen mee te nemen. Zoals de minister terecht aangeeft, is zorgverlening vaak kritieke dienstverlening die niet kan wachten.

Ik deel uw zorgen voor wat betreft digitale afhankelijkheden in de zorg. Echter, het is en blijft de verantwoordelijkheid van de zorgaanbieder om hiervoor handelingsperspectieven op te stellen naar aanleiding op basis van hun individuele risicoafwegingen. Bovendien bevat de norm voor informatiebeveiliging in de zorg (NEN7510) beheersmaatregelen voor het gebruik van clouddiensten. Alle zorgaanbieders zijn verplicht aantoonbaar te voldoen aan deze norm. Om te voldoen aan deze norm dient een organisatie de risico's behorend bij het gebruik van clouddiensten in kaart te hebben gebracht en dient deze ook eventueel benodigde mitigerende maatregelen te nemen.

Deze leden vragen daarom wat de minister van VWS specifiek doet om bij zorg-IT-systemen digitaal autonomer te worden.

Ik deel uw zorgen voor wat betreft digitale afhankelijkheden in de zorg. Echter, het is en blijft de verantwoordelijkheid van de zorgaanbieder om hiervoor handelingsperspectieven op te stellen op basis van hun individuele risicoafwegingen. Uit de verantwoordelijkheid van de zorgaanbieder volgt dat zij zelf de afwegingen zullen maken, passend bij de eigen context. Er bestaat hiervoor namelijk geen '*quick fix*' of '*one size fits all*'. De Rijksoverheid is daarnaast bezig met een herziening van het Rijkscloudbeleid naar aanleiding van recente geopolitieke ontwikkelingen. Na vaststelling van dit nieuwe Rijkscloud beleid zal ik de gesprekken met Cumuluz, als uitvoeringsorganisatie van een landelijk dekkend netwerk, intensiveren om te komen tot een passende en proportionele vertaling van dit rijksbeleid naar de zorg. Uitvoering en implementatie zal daarna tijd kosten, maar het is eerst van belang nieuwe en heldere kaders te schetsen.
Zij vragen of de minister nader wil toelichten waarom hij niet een meer dwingend kader aan de sector wil meegeven.

Ik kan en wil geen dwingend kader voorschrijven aan de zorgsector. Uit de verantwoordelijkheid van de zorgaanbieder volgt dat zij zelf de afwegingen zullen moeten maken, passend bij de eigen context.

Zij vragen wat de minister doet om in het cloudbeleid specifiek aandacht te besteden aan de zorgsector, vanwege het cruciale publieke belang.

In het kader van digitale autonomie verdient de risicoanalyse bij de inzet van cloud-toepassingen bijzondere aandacht omdat die vaak zorgt voor een grotere afhankelijkheid van leveranciers. Waar overwogen wordt om cloud toepassingen in te zetten of al ingezet zijn, adviseer ik om daarvoor het Implementatiekader Risicoafweging Cloudgebruik[15] voor de Rijksoverheid te gebruiken. Dit is een algemeen kader. Dit kader is niet specifiek toegepast op de zorg, maar generiek toepasbaar. Voor het gebruik van de cloud is dit in het bijzonder van belang, aangezien er nog weinig alternatieven beschikbaar zijn

De leden van de CDA-fractie vragen tot slot naar het advies van de Autoriteit Consument & Markt (ACM) over het verbeteren van de zorg-ICT-markt. Deze leden vragen of de minister deelt dat een betere ICT-markt, met minder afhankelijkheid van enkele leveranciers ook bijdraagt aan informatieveiligheid in de zorg. Deze leden vragen of de minister wil ingaan op de aanbevelingen van de ACM uit januari 2025.

De afhankelijkheid van enkele zorg-ICT- leveranciers kan nadelige gevolgen hebben voor de continuïteit van zorg. Zorgaanbieders zijn in de eerste plaats zelf verantwoordelijk voor de informatieveiligheid. Dit is onderdeel van de bedrijfsvoering en zou net zo vanzelfsprekend moeten zijn als andere onderdelen, zoals brandveiligheid van het gebouw en personeel. ICT-uitgaven of investeringen zouden dit belang moeten reflecteren. Zorgaanbieders bepalen welke maatregelen genomen moeten worden en moeten zorgen dat ze de juiste eisen stellen aan hun zorg-ICT-leveranciers. Ik vraag hier in een brief aan koepels en zorgbestuurders die in november gestuurd is aandacht voor.

Op 20 januari 2026 is de Tweede Kamer geïnformeerd over de Voortgang databeschikbaarheid in de zorg[16]. Bij het onderwerp continuïteit van zorg, staat dat ICT-diensten en -infrastructuur steeds vaker cruciaal zijn voor de continuïteit van zorg. Ik werk daarom aan verschillende initiatieven om de continuïteit van zorg-ICT te versterken.

Bij het onderdeel Stand van zaken zorg-ICT-markt van de brief over Voortgang databeschikbaarheid in de zorg, wordt nader ingegaan op het advies van de ACM. In januari vorig jaar heeft de ACM een brief gestuurd aan de toenmalige minister van VWS over de geslotenheid van ICT-systemen, de nadelen hiervan voor de zorg en ook de beperkingen van de instrumenten die de ACM tot haar beschikking heeft om hiertegen op te treden. Vanwege de urgentie van de genoemde problematiek adviseert de ACM om data-openheid wettelijk af te dwingen. Aan de ACM is geantwoord dat de mogelijkheden worden onderzocht voor verplichtstelling van databeschikbaarheid en open datastandaarden. Dit sluit aan bij de motie van het lid Bushoff[17], waarin verzocht wordt ICT-leveranciers in de zorg de komende jaren verplicht worden gebruik te maken van open datastandaarden. In mijn brief ‘stand van zaken landelijk dekkend netwerk’ die ik voor het commissiedebat digitale zorg (gepland op 21 mei) naar uw Kamer zal sturen, zal ik hier dieper op ingaan.

[15] Implementatiekader risicoafweging cloudgebruik, versie 1.1, (CIO Rijk – Interdepartementale Commissie Bedrijfsvoering Rijksdienst), https://open.overheid.nl/documenten/ronl-734f947ec6465e4f75a56bed82fe64a1135f71a8/pdf (5 januari 2023)
[16] *Kamerstukken II*, 2025/2026, 27 529, nr. 355
[17] *Kamerstukken II*, 2024/25, 27 529, nr. 348

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van de brief over informatieveiligheid in de zorg. Genoemde leden hebben geen vragen aan de minister.