Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

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

Bezoekadres
Parnassusplein 5
2511 VX Den Haag
www.rijksoverheid.nl

Kenmerk
4570085-1106423-DICIO

Bijlage(n)

Kenmerk afzender

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

Datum 27 november 2026
Betreft Kamerbrief Digitale en Fysieke weerbaarheid in de Zorg

Geachte voorzitter,

Met deze brief wordt uw Kamer geïnformeerd, mede namens de minister van Volksgezondheid, Welzijn en Sport, over de implementatie in nationale wetgeving van de Europese *Network and Information Security Directive* (NIS2-richtlijn) en de *Critical Entities Resilience Directive* (CER-richtlijn).

De NIS2-richtlijn heeft tot doel de digitale weerbaarheid van organisaties tegen bijvoorbeeld cyberaanvallen te versterken. De CER-richtlijn heeft tot doel de fysieke weerbaarheid van organisaties te versterken die zijn aangewezen als 'kritieke entiteiten' tegen fysieke bedreigingen, zoals natuurrampen of terroristische aanslagen. Onder coördinatie van het ministerie van Justitie en Veiligheid (JenV) zijn deze richtlijnen omgezet in nationale wetten en onderliggende algemene maatregelen van bestuur (AmvB's). Voor de digitale weerbaarheid zijn dit de *Cyberbeveiligingswet (Cbw)* en *het Cyberbeveiligingsbesluit (Cbb) e*n voor de fysieke weerbaarheid zijn dit de *Wet weerbaarheid kritieke entiteiten (Wwke)* en het *Besluit weerbaarheid kritieke entiteiten (Bwke)*. Om de vereisten uit de Cbw en de Wwke en de onderliggende besluiten nader uit te werken voor de zorgsector, heeft de minister van Langdurige Jeugd en Sport (MLJS) de sectorspecifieke ministeriële regeling *Cyberbeveiligingsregeling voor de Zorg (CbrZ)* ingevoerd voor de digitale weerbaarheid. Daarnaast heeft de minister van Volksgezondheid, Welzijn en Sport (MVWS) de sectorspecifieke ministeriële *Regeling weerbaarheid kritieke entiteiten voor de zorg (RwkeZ)* ingevoerd voor de fysieke weerbaarheid.

In deze brief wordt eerst worden ingegaan op *'NIS2 naar Cyberbeveiligingswet'*, dan van *'CER naar Wet weerbaarheid kritieke entiteiten'* en tot slot wordt een aantal toezeggingen afgedaan en wordt gereageerd op enkele moties onder de kopjes, *'De Cbw en de kleine zorgaanbieders', 'Digitale autonomie voor het zorgveld'* en *'Aanbestedingen en informatiebeveiliging'*.

Met deze brief worden de volgende toezeggingen afgedaan en wordt gereageerd op de volgende moties vanuit de Kamer.

- De toezegging van de schriftelijke inbreng op Kamerstuk II 2025/2026, 27529 nr. 353 wordt afgedaan onder *'de Cbw en de kleine zorgaanbieders'*[1].
- Het eerste deel van de motie van leden Bushoff en Kathmann uit Kamerstuk II 2025/2026, 27529 nr. 378 waarin ten eerste wordt opgeroepen de digitale

[1] Schriftelijke inbreng Informatieveiligheid in de zorg op Kamerstuk II 2025/2026, 27529 nr. 353

autonomie van de zorgsector te vergroten en hiervoor samen met het veld plannen te ontwikkelen. Ten tweede wordt gevraagd de afhankelijkheid van (niet-Europese) ICT-bedrijven in kaart te brengen en de resultaten in Q1 2027 met de Kamer te delen. Het tweede deel van de motie vraagt meer tijd en afstemming, daarom wordt in deze brief alleen het eerste deel afgedaan onder het kopje *'Digitale Autonomie voor het zorgveld'*[2].

- De motie uit Kamerstuk II 2025/2026, 32793 nr. 863 over VWS als aanbestedende partij in aanbestedingen voor projecten met grootschalige verwerking van medische gegevens wordt afgedaan onder *'Aanbestedingen en informatiebeveiliging'*[3].
- Naar aanleiding van de vraag van de heer Claassen over kwantumcryptografie en de toezegging om dit onderwerp mee te nemen in de brief over cyber- en informatieveiligheid, wil de minister LJS u erop wijzen dat deze toezegging nog openstaat. Gezien de toenemende urgentie van kwantumcryptografie en de mogelijke consequenties voor de informatieveiligheid, acht de minister LJS het van belang om deze toezegging op korte termijn in te vullen. Ik zal hier uiterlijk in Q1 2027 op terugkomen.

1. Van NIS2 naar Cyberbeveiligingswet

De Europese NIS2-richtlijn is nationaal omgezet in de Cbw en is op 15 augustus jl. van kracht gegaan. Met de invoering van de Cbw wordt de digitale weerbaarheid in alle sectoren, inclusief de gezondheidszorg, verder versterkt. De wet is van toepassing op de sector gezondheidszorg en op de subsector *vervaardigen medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek*. Een organisatie valt binnen de reikwijdte van de wet als zij voldoet aan de criteria voor het aantal fte's óf aan de criteria voor de jaaromzet en het balanstotaal. Op basis van deze criteria wordt ook bepaald of de organisatie belangrijk (50 fte of meer) of essentieel (250 fte of meer) is.[4]

Zorgplicht: NEN 7510 wordt onderdeel van groter geheel

Informatiebeveiliging is niet nieuw voor het zorgveld. Het vormteen cruciaal onderdeel van het dagelijkse werk van zorgverleners. Om informatiebeveiliging in zorgorganisaties te vergroten, geldt er een wettelijke verplichting om te voldoen aan de norm NEN 7510. Deze norm is in 2024 herzien en afgestemd op elementen uit de NIS2-richtlijn. NEN 7510 is een belangrijk instrument voor het waarborgen van digitale veiligheid in de zorg en richt zich op het beveiligen van persoonlijke gezondheidsinformatie door zorgaanbieders. Naleving ervan draagt direct bij aan veiligere zorg. Entiteiten die onder de reikwijdte van de Cbw vallen, moeten een aantal verplichtingen uit de wet naleven: de zorgplicht, de meldplicht, de registratieplicht en de informatieplicht. Met de uitwerking van de zorgplicht in de Cyberbeveiligingsregeling voor de Zorg heeft het kabinet rekening gehouden met bestaande normenkaders zoals NEN 7510 en de internationaal erkende standaard ISO 27001.

De Cbw gaat verder dan alleen het implementeren van deze norm. De Cbw ziet ook op meerdere (sub)sectoren. De zorgplicht verplicht entiteiten niet alleen hun eigen informatiebeveiliging op orde te hebben, maar ook actief te toetsen op ketenveiligheid. Hierdoor wordt informatiebeveiliging breder aangepakt. NEN 7510 is niet meer alleen een aparte eis waaraan organisaties moeten voldoen. Het wordt onderdeel van een groter systeem voor het beheersen van risico's. Denk hierbij aan het uitvoeren van een risicoanalyse voor het in kaart brengen van de risico's op netwerk- en informatiesystemen binnen een organisatie. Samen met de andere wettelijke

[2] Kamerstukken II 2025/2026, 27529 nr. 378

[3] Kamerstuk II 2025/2026, 32793 nr. 863

[4] Zorgsector en de Cbw | Data voor gezondheid

verplichtingen uit de Cbw zorgt dit ervoor dat informatiebeveiliging geen eenmalig doel is, maar een continu proces binnen de organisatie.

Meldplicht: vaststelling drempelwaarden en aanwijzing Z-CERT
Om invulling te geven aan de meldplicht heeft het kabinet in de Cyberbeveiligingsregeling voor de Zorg sectorspecifieke drempelwaarden vastgesteld. Deze drempelwaarden geven de entiteiten die onder de Cbw vallen handvatten voor de bepaling wat een significant incident is en wanneer deze gemeld moet worden. Het belang van de meldplicht ligt in het sneller identificeren van kwetsbaarheden en risico's voor de entiteit zelf en de rechtstreekse keten.

Significante incidenten moeten binnen 24 uur gemeld worden in het meldportaal van het Nationaal Cyber Security Centrum (NCSC). Entiteiten die onder de reikwijdte van de wet vallen, hebben recht op ondersteuning van een Computer Security Incident Response Team (CSIRT) bij significante incidenten. Na overleg met de Algemene Rekenkamer heeft het kabinet Z-CERT aangewezen als sectoraal CSIRT (sCSIRT) voor het zorgveld. Met de aanwijzing als sCSIRT is Z-CERT een rechtspersoon met een wettelijke taak (RWT) en zal het voor het uitvoeren van de wettelijke taken worden bekostigd. Om de entiteiten te ondersteunen met de implementatie van de Cbw zijn er hulpmiddelen beschikbaar in de vorm van informatie, Q&A's en animaties.[5]

2. Van CER naar Wet weerbaarheid kritieke entiteiten

De Europese CER-richtlijn is nationaal omgezet in de Wwke en is op 15 augustus jl. van kracht gegaan. Het doel van de Wwke is om de essentiële diensten binnen Nederland zo goed mogelijk te beschermen tegen allerlei soorten dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen. Deze essentiële diensten zijn gekoppeld aan zogeheten 'kritieke entiteiten' en mogen ten tijde van een ramp niet omvallen. Kritieke entiteiten die aangewezen worden, worden niet openbaar gemaakt vanwege de gevoeligheid. Deze lijst is gerubriceerd als *Staatsgeheim-Confidentieel*.

Extra categorieën die als kritieke entiteit kunnen worden aangewezen
De Wwke is onder andere van toepassing op de sector gezondheidszorg en verdeelt die sector in een aantal categorieën[6]. Daarnaast biedt de Wwke de mogelijkheid om binnen die sector aanvullende categorieën aan te wijzen.
De minister van VWS heeft van die mogelijkheid gebruik gemaakt en de volgende extra categorieën toegevoegd:

- aanbieders van systemen of diensten voor de beschikbaarheid en elektronische uitwisseling van gegevens, waaronder gegevens over de gezondheid en andere persoonsgegevens, ten behoeve van de zorg voor een patiënt, en;
- entiteiten gericht op de toepassing van bloedproducten of lichaamsmateriaal op de mens.

Dit is gedaan omdat het leveren van zorg afhankelijk kan zijn van ondersteunende diensten voor de zorg, die nu niet onder de reikwijdte van de Wwke vallen. Om de continuïteit van de gezondheidszorg te versterken, is het noodzakelijk om ook de mogelijkheid te hebben om dergelijke cruciale partijen in de zorgketen als 'kritieke entiteit' aan te kunnen wijzen onder de Wwke.
Aanwijzing kritieke entiteiten en periodieke herziening van de risicobeoordeling

[5] Cyberbeveiligingswet | Data voor gezondheid

[6] Zorgaanbieders, EU-referentielaboratoria, Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen, Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen, Entiteiten die medische hulpmiddelen vervaardigen in noodsituaties, Entiteiten die houder zijn van een groothandelsvergunning

Als bevoegde autoriteit voor de sector gezondheidszorg heeft de minister van VWS een sectorale risicobeoordeling uitgevoerd. De sectorale risicobeoordeling dient twee doelen: Ten eerste stelt deze een dreigingsbeeld voor de sector gezondheidszorg op, die kritieke entiteiten als basis kunnen gebruiken voor hun eigen risicobeoordeling. Ten tweede identificeert de beoordeling welke diensten binnen de gezondheidszorg zó essentieel zijn dat uitval of verstoring tot ernstige gezondheidsschade leidt.

Aan de hand van de sectorale risicobeoordeling en de criteria uit de Regeling weerbaarheid kritieke entiteiten voor de zorg heeft de minister van VWS een aantal kritieke entiteiten aangewezen, deze aanwijzing moest vóór 15 september 2026 gebeuren. Gezien het snel veranderende dreigingslandschap zal de risicobeoordeling minstens elke vier jaar óf zodra hier aanleiding toe is geëvalueerd en herzien worden. Na 15 september 2026 kunnen extra kritieke entiteiten worden geïdentificeerd en aangewezen, dit zal gelden voor de extra categorie *'aanbieders van systemen of diensten voor de beschikbaarheid en elektronische uitwisseling van gegevens, waaronder gegevens over de gezondheid en andere persoonsgegevens, ten behoeve van de zorg voor een patiënt'*. Zodra entiteiten uit deze categorie zijn geïdentificeerd en aangewezen, worden ze toegevoegd aan de lijst van kritieke entiteiten en dus niet openbaar gemaakt. De lijst met aangewezen kritieke entiteiten is gezien de gevoeligheid gerubriceerd als *Staatsgeheim-Confidentieel* en wordt dus niet openbaar gemaakt.

Plichten Wwke
Kritieke entiteiten zijn verplicht om binnen tien maanden na aanwijzing passende en evenredige maatregelen te nemen om risico's voor hun organisatie te beperken en de weerbaarheid van hun essentiële diensten te vergroten. De zorgplicht is uitgewerkt in de Wwke en nader gespecifieerd in de bijbehorende AMvB, het Besluit weerbaarheid kritieke entiteiten (Bwke). Hieronder valt bijvoorbeeld het identificeren van kritieke infrastructuur, het nemen van maatregelen om gebouwen en kritieke infrastructuur te beschermen en het opstellen en periodiek evalueren van crisisbeheersings- en bedrijfscontinuïteitsplannen.

De meldplicht houdt in dat kritieke entiteiten incidenten die hun dienstverlening aanzienlijk (kunnen) verstoren binnen 24 uur moeten melden in het meldportaal van het Nationaal Cyber Security Centrum (NCSC). Dit helpt om de impact voor de bredere gezondheidszorg in te schatten en waar mogelijk actie te ondernemen om organisaties binnen de gezondheidszorg te waarschuwen door middel van informatie-uitwisseling.

Onderzoek naar mogelijke ondersteuning
Hoewel het in eerste instantie aan organisaties zélf is om hun weerbaarheid te versterken en aan de verplichtingen uit de Wwke te voldoen, zal de minister van VWS tegelijkertijd als bevoegde autoriteit de mogelijkheden verkennen om kritieke entiteiten binnen de zorg te ondersteunen. Deze ondersteuning zal voornamelijk bestaan uit het stimuleren van samenwerking en informatiedeling tussen kritieke entiteiten, de keten en het ministerie. De ondersteuning voorziet echter niet in het beschikbaar stellen van financiële middelen.

3. Toezicht op naleving Cbw en Wwke

De Inspectie Gezondheidszorg en Jeugd (IGJ) is de toezichthouder voor de sector gezondheidszorg in het kader van de Cbw en Wwke. Voor het toezichthouden in het kader van de Cbw en de Wwke bekostigt mijn ministerie de IGJ structureel.
Voor de Cbw zal de IGJ-toezicht houden op de belangrijke en essentiële entiteiten uit de Cbw. Het toezicht door de IGJ wordt vormgegeven op basis van risicoafwegingen. Dit betekent dat niet alle incidentmeldingen automatisch leiden tot nader onderzoek. Daarnaast kan er steekproefsgewijs proactief toezicht worden ingezet bij essentiële entiteiten.

Voor de Wwke wordt er toezicht gehouden op de kritieke entiteiten; dit kan zowel proactief als naar aanleiding van signalen. Dit vindt in het algemeen plaats nadat de kritieke fase van het incident is afgerond. De hoogste prioriteit bij een incident is voortzetting van de essentiële dienst.

4. De Cbw en de kleine zorgaanbieders

Ook voor kleine zorgaanbieders die niet onder de Cbw vallen, is informatiebeveiliging van groot belang. Daarom blijft het belangrijk dat ook kleine zorgaanbieders voldoen aan de norm NEN 7510, zodat de vertrouwelijkheid, integriteit en beschikbaarheid van patiëntgegevens goed worden beschermd.
Voor de kleine zorgaanbieder zijn hulpmiddelen beschikbaar, die zijn benoemd in de Kamerbrief over informatieveiligheid in de zorg[7]. Mijn ministerie is met de kleine zorgaanbieders in gesprek over de vraag hoe deze groep aanvullend ondersteund kan worden.

De Inspectie Gezondheidszorg en Jeugd (IGJ) merkt in haar onderzoek naar belemmeringen bij de informatieveiligheid van kleine zorgaanbieders[8] op dat er een divers en versplinterd aanbod is van hulpmiddelen voor het verhogen van de informatiebeveiliging van de zorg. Mijn ministerie zal daarom alle beschikbare hulpmiddelen bijeenbrengen in een overzicht en dit publiceren op de website 'Data voor gezondheid'[9]. Hiermee wordt de toegankelijkheid en bekendheid van deze hulpmiddelen vergroot.

5. Digitale autonomie voor het zorgveld

De zorg digitaliseert in hoog tempo en wordt hiermee steeds meer afhankelijk van verschillende digitale systemen en leveranciers. In de context van de huidige geopolitieke ontwikkelingen brengen deze afhankelijkheden aanvullende risico's met zich mee. Het is daarom van belang dat de zorg haar digitale autonomie vergroot. Dit houdt onder meer in dat strategische afhankelijkheden verminderd worden en technologische zelfredzaamheid versterkt wordt[10].

Mijn ambtsvoorganger heeft de zorgsector in de Kamerbrief over informatieveiligheid in de zorg[11] opgeroepen de afhankelijkheid van leveranciers mee te nemen in hun risicoafwegingen. Het maken van een risicoafweging is verplicht in het kader van NEN 7510, de norm voor informatiebeveiliging in de zorg. De verantwoordelijkheid hiervoor ligt bij zorgorganisaties. Elke organisatie moet een risicoanalyse uitvoeren. Onderdeel hiervan is onder andere het vaststellen van kritieke processen en afhankelijkheden om vervolgens een geïnformeerde keuze te maken, bijvoorbeeld over de looptijd van contracten, het toepassen van extra beveiligingslagen of de mogelijkheid om van leveranciers of systeem te wisselen.

Initiatieven voor meer grip

Mijn ministerie onderneemt samen met het veld verschillende initiatieven om meer grip te krijgen op het thema digitale autonomie. Ten eerste organiseert mijn ministerie in het

[7] Kamerstukken II, 2025/26, 27529 nr. 353

[8] Rapport over informatiebeveiliging bij kleine zorgaanbieders, IGJ, 03-07-2025.

[9] Data voor gezondheid | Data voor gezondheid

[10] Visie Digitale autonomie en soevereiniteit van de overheid

[11] Kamerstukken II, 2025/26, 27529 nr. 353

najaar van 2026 een expertsessie met vertegenwoordigers van koepels, brancheorganisaties en zorgorganisaties. Het doel van deze sessie is het kennis- en bewustzijnsniveau te verhogen, de dialoog te voeren over eventuele handelingsperspectieven en samenwerking tussen de deelnemende partijen te vergroten om de afhankelijkheid te verkleinen.
Ten tweede heeft mijn ministerie aan het Nederlands Normalisatie Instituut (NEN) middelen verstrekt voor onder andere het ontwikkelen van een hulpmiddel bij de onder de norm NEN 7510 verplichte risicoanalyse. Dit hulpmiddel is kosteloos beschikbaar en helpt zorginstellingen bij het doorlopen van het gehele risicoanalyseproces om te komen tot bij de eigen context passende beheersmaatregelen.

Ten derde kan de zorg leren van ervaringen uit andere sectoren. Hier wordt bijvoorbeeld gedacht aan grote gemeenten, banken en de universiteiten. De *best practices* en geleerde lessen kunnen inspirerend werken voor de zorgsector. Daarom worden in het komende kwartaal gesprekken gevoerd met (semi)publieke en private organisaties die stappen vooruitzetten op gebied van digitale soevereiniteit zoals universiteiten, banken en grote gemeenten. Geleerde lessen zal worden gedeeld met het zorgveld.

In de eerdergenoemde Kamerbrief over informatieveiligheid in de zorg is geadviseerd om gebruik te maken van het *Implementatiekader risicoafweging cloudgebruik.* Mijn ministerie heeft een impactanalyse voor de zorg van het recent gepubliceerde herziene *Rijkscloudbeleid*[12] uitgevoerd. Op basis van deze impactanalyse is besloten geen aanvullend zorgspecifiek kader voor cloudbeleid te stellen. In de bestaande kaders liggen namelijk al voldoende eisen besloten om de risico's van het gebruik van cloudtoepassingen (zoals bijvoorbeeld afhankelijkheid van een beperkt aantal leveranciers) tegen te gaan. Om de zorg te ondersteunen bij dit complexe vraagstuk wordt ingezet op een communicatiestrategie met onder andere praktische hulpmiddelen voor veilige en verantwoorde inzet van cloudtoepassingen in de zorg.[13]

Tot slot wil mijn ministerie aan het zorgveld uitdragen dat er inmiddels (Europese) alternatieven zijn voor belangrijke ICT-componenten. Het uitgangspunt van open source ontwikkeling van het Gezondheidsinformatiestelsel is ook een antwoord op leveranciers specifieke beperkingen, onderdeel van de brede aanpak naar meer digitale autonomie.

6. Aanbestedingen en informatiebeveiliging

In de situaties waarvoor VWS de aanbestedende partij is, geldt de Aanbestedingswet 2012, die binnen het departement standaard wordt toegepast. Wanneer medische gegevens en persoonsgegevens beschermd dienen te worden zijn er procedures aanwezig om de organisatie te ondersteunen met het stellen van de juiste voorwaarden volgens de BIO2. De BIO2 is de overheid brede norm die ook gebruikt moet worden voor inkoop trajecten, zodat de leveranciers de juiste maatregelen kunnen implementeren. Hierin ondersteunt de Chief Information Security Officer (CISO) inhoudelijk met het opstellen van de juiste risicoanalyses en het pakket van maatregelen.

7. Tot slot: meer bewustzijn vergroot de weerbaarheid

De Cbw en de Wwke versterken de digitale en fysieke weerbaarheid van onder meer onze gezondheidszorg. Dat doen deze wetten allereerst door hogere eisen te stellen aan de beveiliging van organisaties, maar ook door te zorgen voor meer bewustzijn. Want door organisaties te verplichten om dreigingen en risico's in kaart te brengen, krijgen ze meer inzicht in blinde vlekken en verbeterpunten.

---

[12] Kamerstukken II, 2025/26, 26643 nr. 1541

[13] Implementatiekader risicoafweging cloudgebruik, versie 1.1, (CIO Rijk – Interdepartementale Commissie Bedrijfsvoering Rijksdienst), https://open.overheid.nl/documenten/ronl734f947ec6465e4f75a56bed82fe64a1135f71a8/pdf (5 januari 2023)

De combinatie van digitale en fysieke weerbaarheid biedt zorgorganisaties een robuustere verdedigingslijn tegen uiteenlopende bedreigingen. Deze gelaagde benadering erkent dat informatiebeveiliging niet alleen een IT-kwestie is, maar onderdeel van het algehele operationele risicobeheer, en dus aandacht vereist op meerdere niveaus van de organisatie. De continuïteit van zorg vraagt in tijden van hogere dreigingsniveaus een hogere weerbaarheid.

Hoogachtend,

de minister van Langdurige Zorg,
Jeugd en Sport,

Mirjam Sterk