



> Retouradres Postbus 20350 2500 EJ Den Haag

Bezoekadres

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

Kenmerk

4237644-1089675-DICIO

Kenmerk afzender

Bijlage(n)

1

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

04 DEC 2025

Datum

Betreft Bestuurdersbrief informatieveiligheid

Geachte heer/mevrouw,

Met deze brief verzoek ik u als zorgbestuurder mede verantwoordelijkheid te nemen voor de digitale weerbaarheid van de zorgsector. Tevens wil ik u ondersteunen met handvatten om binnen uw organisatie zelf hiermee aan de slag te gaan en de benodigde versnelling te realiseren. Uw rol hierin is cruciaal, omdat u binnen uw organisatie de prioriteiten stelt.

Deze brief wordt tegelijkertijd verstuurd met een Kamerbrief waarin ik de Tweede Kamer informeer over ontwikkelingen op het gebied van informatiebeveiliging in de zorgsector.

Waarom deze brief?

De zorgsector maakt de beweging naar databeschikbaarheid: de juiste gegevens, op het juiste moment, op de juiste plek. Dat vraagt om vertrouwen in gegevens en systemen en het verantwoorde gebruik daarvan. In de huidige geopolitieke context is een hoge mate van digitale weerbaarheid nodig tegen cyberdreigingen die dat vertrouwen kunnen ondermijnen.

De hack bij het laboratorium Clinical Diagnostics, met een groot datalek tot gevolg waarbij onder andere de persoonsgegevens van honderdduizenden deelnemers aan het bevolkingsonderzoek baarmoederhalskanker zijn buitgemaakt, heeft enorme impact op patiënten, organisaties en het vertrouwen in data in de zorg. Die aanval maakt opnieuw duidelijk hoe kwetsbaar de zorgsector is en wat we te beschermen hebben. Uit het dreigingsbeeld¹ van het expertisecentrum cybersecurity in de zorg (Z-CERT) wordt duidelijk dat zorginstellingen steeds vaker het doelwit worden van cyberaanvallen. En uit rapporten van de Inspectie, Gezondheid en Jeugd (IGJ) blijkt dat veel zorgorganisatie nog steeds niet aan de norm voor informatiebeveiliging in de zorg, NEN 7510, voldoen. De Tweede Kamer heeft ook aangedrongen op een intensivering van de inspanningen.

Kortom, er staat ons iets te doen. En we zijn er allemaal medeverantwoordelijk voor dat deze opgave slaagt.

¹ [Dreigingsbeeld Z-CERT 2024](#)



Wat vragen we van u?

Het is belangrijk dat alle zorgorganisaties in de keten zich bewust zijn van de informatiebeveiligings- en privacy risico's en dat zij de juiste maatregelen implementeren om dat soort incidenten te voorkomen.

Kenmerk
4237644-1089675-DICIO

Organisaties moeten voldoen aan wetgeving en kaders zoals de Algemene verordening gegevensbescherming (AVG), NEN 7510 en vanaf naar verwachting het tweede kwartaal van 2026, de Cyberbeveiligingswet (Cbw).² NEN 7510 en de Cbw sluiten grotendeels op elkaar aan. Organisaties die nu al aan NEN 7510 voldoen, zijn daarmee al een stap in de goede richting naar naleving van de Cbw.

Digitale weerbaarheid is een gezamenlijke verantwoordelijkheid van de gehele zorgketen. Dit is geen gemakkelijke opgave, zeker voor kleinere organisaties. Gelukkig zijn er diverse hulpmiddelen beschikbaar die u kunt raadplegen via de bijgevoegde QR-code.

Voor een aantal vaak wat onderbelichte inhoudelijke aandachtspunten rondom informatiebeveiliging en privacybescherming wil ik hier in het bijzonder uw aandacht vragen:

- Digitale weerbaarheid draait om meer dan techniek, het vraagt ook om investeringen in bewustwording, processen en gedrag.
- Vergeet uw leveranciersketen niet. Heeft u met uw leveranciers de juiste afspraken gemaakt?
- Informatiebeveiliging is geen project, maar een continu proces van aanpassen aan gewijzigde dreigingen en technische mogelijkheden, evalueren en bijsturen.
- Wees u ervan bewust dat er onder de Cbw een bestuurlijke aansprakelijkheid wordt geïntroduceerd voor bestuurders.

Ik wil afsluiten met drie boodschappen:

1. Denk niet 'het zal ons niet overkomen', maar stuur erop dat de organisatie leert van incidenten die zich elders al hebben voorgedaan. In het dreigingsbeeld van Z-CERT vindt u voorbeelden van incidenten én adviezen over welke acties u kunt ondernemen.
2. Informatiebeveiliging en privacybescherming zijn geen keuzes die ook een onsje minder kunnen. Patiënten en burgers verdienen die digitale zorgvuldigheid in het kader van patiëntveiligheid en continuïteit van zorg. Dat moet net zo vanzelfsprekend zijn als het slot op de deur, de hygiënische maatregelen en de brandtrap in uw organisatie.
3. Het is aan u om de handschoenen op te pakken en te voldoen aan de wettelijke kaders. Maar weet ook dat u er daarbij niet alleen voor staat. Er zijn talloze hulpmiddelen om u hierbij te ondersteunen, zoals ook al eerder genoemd in deze brief en die te vinden zijn via de bijgevoegde QR-code.

² De Cyberbeveiligingswet is de omzetting in nationale wetgeving van de Europese *Network and Information Security Directive* (NIS2).



Ik vertrouw erop dat u hiermee aan de slag gaat, zo zorgen we samen voor een digitaal weerbare zorgsector.

Hoogachtend,

de minister van Volksgezondheid,
Welzijn en Sport,

Jan Anthonie Bruijn

Kenmerk
4237644-1089675-DICIO