



FACTSHEET

NEN 7510:2024

De NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg.

In 2024 is een nieuwe versie gepubliceerd.

Deze vervangt de NEN 7510:2017 en sluit beter aan op actuele cyberdreigingen, strengere toezichtseisen en Europese regelgevingen zoals NIS2.

Voor zorgorganisaties is NEN 7510 geen vrijblijvende richtlijn, maar een norm waaraan zij moeten voldoen.

Wanneer is **NEN 7510:2024** relevant of vereist?

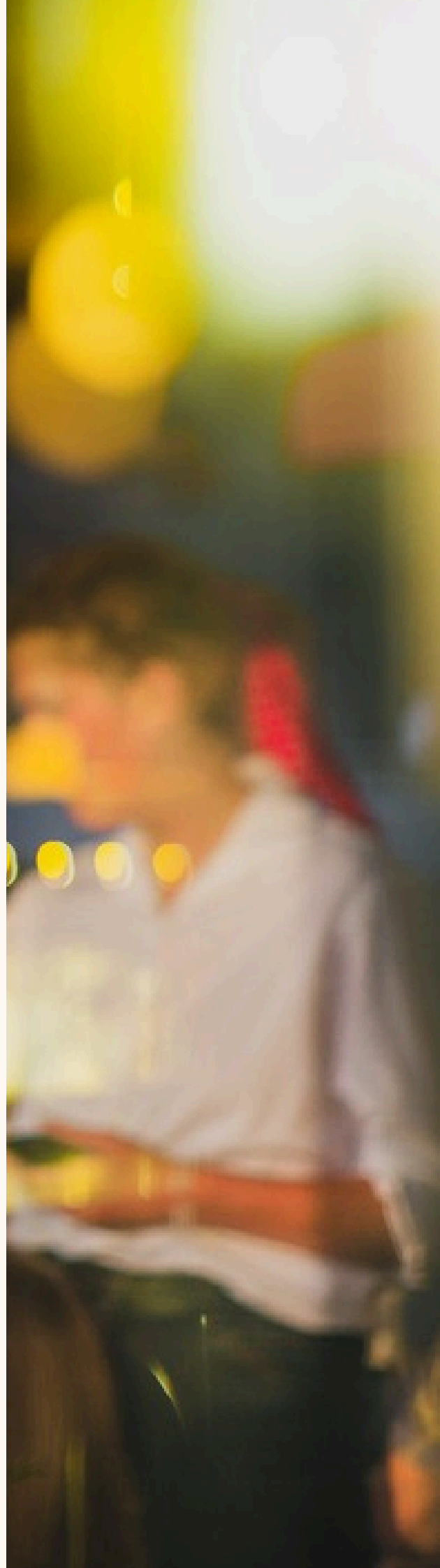
Verwerkt jouw organisatie gezondheidsdata? Dan moet je voldoen aan strengere wettelijke beveiligingseisen uit artikel 32 AVG. NEN 7510:2024 is in Nederland de gangbare norm om aan deze eisen te voldoen, maar is niet in alle gevallen rechtstreeks verplicht.

Deze verplichting tot passende informatiebeveiliging volgt uit wet- en regelgeving over het elektronisch verwerken en uitwisselen van gezondheidsgegevens en het BSN door zorgaanbieders, waaronder de AVG en zorgspecifieke wetgeving, zoals de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en het Besluit elektronische gegevensverwerking door zorgaanbieders. In de praktijk wordt NEN 7510 als gangbare en erkende norm om invulling te geven aan deze beveiligingsverplichtingen in de zorg.

De norm is van toepassing op onder meer:

- Zorgaanbieders (zoals ziekenhuizen, GGZ-instellingen en andere zorginstellingen)
- Ondersteunende organisaties in de zorgketen voor zover zij gezondheidsgegevens verwerken.
- ICT-leveranciers en dienstverleners die een elektronisch uitwisselingssysteem voor zorgaanbieders beheren en in stand houden, en daarbij verantwoordelijk zijn voor de beschikbaarheid, beveiliging en werking van dat systeem.

Voor ICT-leveranciers en andere dienstverleners geldt NEN 7510 niet automatisch als een rechtstreekse wettelijke verplichting. Wel is de norm voor hen direct relevant, omdat zorgaanbieders op grond van wetgeving en toezichtseisen beveiligings- en compliance-eisen stellen aan hun ketenpartners, bijvoorbeeld via contracten en verwerkersovereenkomsten.



Wat vraagt **NEN 7510:2024** van organisaties?

NEN 7510:2024 vereist dat organisaties aantoonbaar grip hebben op hun informatiebeveiliging. Het gaat niet om losse maatregelen maar om een samenhangend structureel beveiligingsniveau.

De norm stelt onder meer eisen aan:

- **Risicomanagement:**
het structureel identificeren en beheersen van risico's voor gezondheidsinformatie
- **Governance en verantwoordelijkheid:**
duidelijke rollen, verantwoordelijkheden en actieve betrokkenheid van het management
- **Toegangsbeveiliging**
Passende autorisaties, logging en controle op toegang tot systemen en gegevens
- **Incident- en business continuity management:**
Heldere procedures voor het herkennen, melden en afhandelen van beveiligingsincidenten.
- **Keten- en leveranciersbeveiliging:**
Beheersing van risico's bij uitbesteding en samenwerking met derden.
- **Bewustwording:**
Medewerkers moeten weten wat van hen wordt verwacht en regelmatig worden getraind.

De 2024-versie legt nadruk op continue verbetering en actuele dreigingen, zoals ransomware en ketenafhankelijkheden.



Overgang van **NEN 7510:2017** naar **2024**

DEADLINE:

Uiterlijk 20 februari 2027 moet een organisatie een transitieaudit hebben afgerond naar NEN 7510:2024.

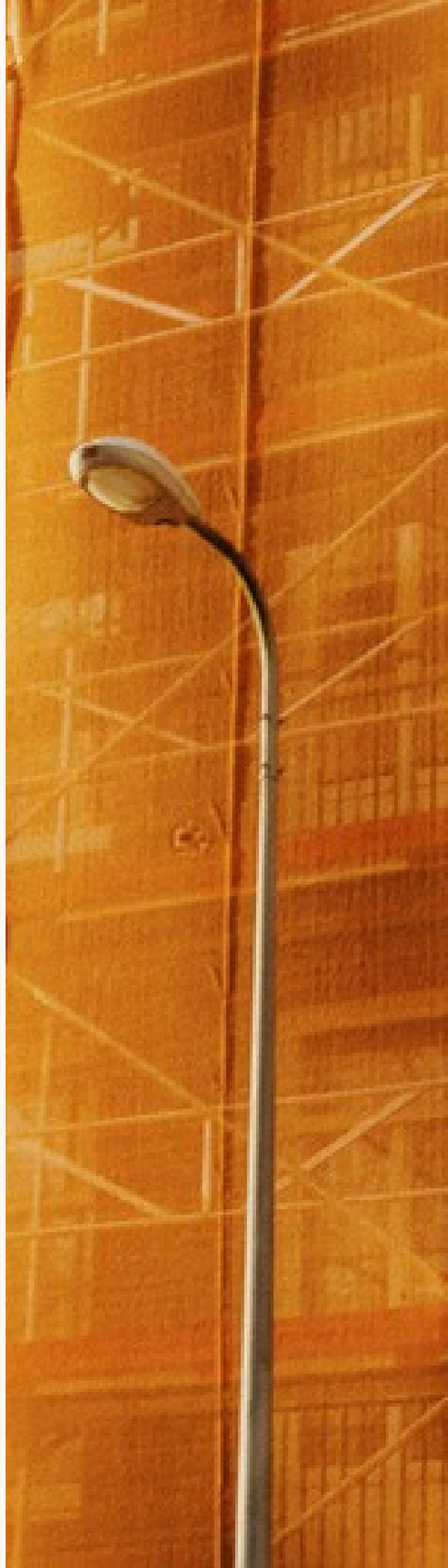
Na deze datum is certificering tegen NEN 7510:2017 niet langer mogelijk. Dit geldt voor organisaties die beschikken over een formeel NEN 7510-certificaat of dit willen behouden. Voor organisaties die NEN 7510 toepassen als referentiekader binnen andere audit- of accreditatiestelsels vervalt geen certificaat, maar ligt het wel in de rede dat zij aansluiten bij de actuele versie van de norm. In alle gevallen is tijdige voorbereiding essentieel om compliance- en continuïteitsrisico's te voorkomen en om aantoonbaar te blijven voldoen aan wettelijke en toezichteisen.

Meer **toezicht** door **AP** en **IGJ**

Het toezicht op informatiebeveiliging in de zorg wordt steeds intensiever. Zowel de Autoriteit Persoonsgegevens (AP) als de Inspectie Gezondheidszorg en Jeugd (IGJ) controleren nadrukkelijker op:

- Structurele informatiebeveiliging
- Aantoonbare maatregelen
- Aantoonbaar voldoen aan NEN 7510

Onvoldoende naleving kan leiden tot handhaving, boetes en reputatieschade.



NEN 7510:2024 en NIS2

De NIS2-richtlijn introduceert een expliciete zorgplicht voor cybersecurity voor veel zorgorganisaties.

Keyfact

Key Fact: De Ministeriële regeling van VWS voor de Cyberbeveiligingswet zegt dat als je voldoet aan NEN 7510:2024 dat dit betekent dat je voldoet aan de Zorgplicht uit NIS2/Cbw. Daarmee voldoe je uiteraard niet aan de overige elementen uit NIS2.

De norm biedt een concreet en erkend kader om aan te tonen dat passende beveiligingsmaatregelen zijn getroffen.

Wat betekent dit concreet

NEN 7510:2024 is geen papieren verplichting, maar een essentieel instrument om te voldoen aan wetgeving, toezicht eisen en contractuele verplichtingen. Tijdig aan de slag gaan met de nieuwe norm versterkt niet alleen de informatiebeveiliging, maar ook de juridische positie van de organisatie.



Zou je extra informatie willen ontvangen?

Vragen over NEN 7510:2024 of de overstap vanuit de 2017 versie?

Wij helpen bij het bepalen van de toepasselijkheid, de transitie naar de nieuwe norm en de voorbereiding op audits en toezicht.

Neem contact op via:
e-mail: contact@ictrecht.nl
telefoonnummer: 020 663 19 41.