GIDS

De complete gids voor NEN 7510 implementatiebegeleiding

Informatiebeveiliging in de zorg: kosten, proces, deadlines en hoe je de juiste begeleider kiest.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij •

Wat is NEN 7510? 1

Waarom is het belangrijk? 2

Hoe werkt implementatie? 3

Wat kost het? 4

Waar moet je op letten? 5

Veelgemaakte fouten 6

NIS2 en regelgeving 7

NEN 7510 vs ISO 27001 8

Trends 2025--2026 9

Aan de slag 10

Bronnenlijst •

Kerncijfers op een rij

De belangrijkste cijfers over NEN 7510 implementatie, kosten en deadlines.

12–18 mnd
Gemiddelde implementatieduur NEN 7510 voor de meeste zorginstellingen
RisGuard [1]

EUR 15–25K
Kosten implementatiebegeleiding voor een kleine zorginstelling (tot 50 mdw)
RisGuard [1]

EUR 5–15K
Kosten certificeringsaudit door een certificerende instelling
BMGRIP [2]

20 feb 2027
Deadline: alleen NEN 7510:2024 certificaten zijn nog geldig
Cuccibu [3]

6
Geaccrediteerde certificerende instellingen voor NEN 7510 in Nederland
NEN [4]

EUR 270K
Gemiddelde schade per cyberincident voor MKB in Nederland
Apex Security [5]

EUR 10M
Maximale NIS2-boete voor essentieel entiteiten (zorg is essentieel sector)
Digitale Overheid [6]

121+
Unieke ransomware-incidenten in Nederland in 2024
NCSC [7]

1. Wat is NEN 7510?

NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg. De norm beschrijft eisen voor het opzetten en onderhouden van een informatiebeveiligingsmanagementsysteem (ISMS) specifiek gericht op de bescherming van persoonlijke gezondheidsinformatie.

De norm is gebaseerd op ISO 27001, maar bevat aanvullende maatregelen die specifiek zijn voor de zorgsector. In december 2024 is NEN 7510:2024 gepubliceerd, die volledig is geharmoniseerd met ISO 27001:2022 [3].

Implementatiebegeleiding is een dienst waarbij een externe consultant je zorginstelling begeleidt bij het volledige traject: van nulmeting tot certificering. De begeleider helpt bij het opzetten van het ISMS, het uitvoeren van de risicoanalyse, het implementeren van maatregelen en de voorbereiding op de certificeringsaudit.

> **Wettelijke verplichting:** Zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie zijn wettelijk verplicht om aantoonbaar aan NEN 7510 te voldoen (IGJ). Certificatie is niet verplicht, maar is de meest gangbare manier om dit aan te tonen [8].

2. Waarom is het belangrijk?

Informatiebeveiliging in de zorg is niet optioneel. Patientgegevens behoren tot de meest gevoelige data die er is.

De zorgsector is een van de sectoren met de meeste cyberaanvallen [9]. Espionage-gemotiveerde aanvallen op de zorgsector stijgen [9]. Een datalek met patientgegevens schaadt niet alleen de financien, maar ook het vertrouwen van patienten en ketenpartners.

De Inspectie Gezondheidszorg en Jeugd (IGJ) handhaaft op naleving van NEN 7510 [8]. Met de komst van de Cyberbeveiligingswet (NIS2) wordt de zorg als essentieel sector aangemerkt, met boetes tot EUR 10 miljoen [6].

3. Hoe werkt implementatie?

Het implementatieproces volgt de PDCA-cyclus (Plan-Do-Check-Act).

1 Nulmeting en gap analysis

2-4 WEKEN

Huidige situatie in kaart brengen en vergelijken met NEN 7510:2024 eisen. Prioriteiten bepalen op basis van risico.

2 Risicoanalyse

3-6 WEKEN

Informatieassets identificeren, dreigingen en kwetsbaarheden beoordelen, risicobehandelingsplan opstellen. NEN biedt een kosteloze Risicotool aan [10].

3 ISMS opzetten en maatregelen implementeren

3-6 MAANDEN

Informatiebeveiligingsbeleid, procedures en werkinstructies opstellen. Beheersmaatregelen selecteren en implementeren.

4 Training en bewustwording

2-4 WEKEN

Medewerkers trainen in informatiebeveiliging en hun rol daarin. Bewustwording creeren over phishing, wachtwoordbeleid en incidentmelding.

5 Interne audit en certificering

4-8 WEKEN

Interne audit uitvoeren, management review houden, corrigerende acties doorvoeren. Dan de certificeringsaudit door een CI: Stage 1 (documentatie) en Stage 2 (praktijk).

4. Wat kost het?

De kosten varieeeren sterk per organisatiegrootte en bestaand volwassenheidsniveau.

ORGANISATIEGROOTTE	CONSULTANCY	CERTIFICERING	TOTAAL 1E JAAR
Klein (huisarts, fysiotherapeut)	EUR 5.000 - 12.000 [1]	EUR 5.000 - 8.000	EUR 10.000 - 20.000
Kleine zorginstelling (tot 50 mdw)	EUR 15.000 - 25.000 [1]	EUR 5.000 - 15.000 [2]	EUR 20.000 - 40.000
Middelgroot (50-250 mdw)	EUR 25.000 - 50.000 [1]	EUR 8.000 - 15.000	EUR 33.000 - 65.000
Groot (ziekenhuis)	EUR 50.000 - 100.000+ [1]	EUR 10.000 - 25.000	EUR 60.000 - 125.000+

Jaarlijkse surveillance-audits kosten EUR 2.000 - 8.000 [2]. Het certificaat is 3 jaar geldig.

5. Waar moet je op letten?

Selectiecriteria voor het kiezen van een implementatiebegeleider.

- **Ervaring met NEN 7510 specifiek** -- Niet alleen ISO 27001, maar de zorgspecifieke eisen
- **Ervaring in jouw type zorginstelling** -- Een ziekenhuis is anders dan een huisartsenpraktijk
- **Pragmatische aanpak** -- Het ISMS moet werkbaar zijn, geen papieren tijger
- **Kennisoverdracht** -- Na het traject moet je het ISMS zelf kunnen onderhouden
- **Onafhankelijk van de CI** -- De begeleider mag niet ook de audit uitvoeren

10 VRAGEN VOOR JE BEGELEIDER

1. Hoeveel NEN 7510 trajecten heb je begeleid in mijn type zorginstelling?
2. Wat is het slagingspercentage bij de eerste certificeringsaudit?
3. Hoe ziet het stappenplan eruit en wat is de doorlooptijd?
4. Wat is de vaste projectprijs en wat is inbegrepen?
5. Wie is mijn vaste contactpersoon tijdens het traject?
6. Hoe zorgen jullie dat het ISMS werkbaar blijft voor mijn team?
7. Begeleiden jullie ook de certificeringsaudit zelf?
8. Wat gebeurt er als we niet slagen bij de eerste audit?
9. Bieden jullie ook nazorg en onderhoud na certificering?
10. Kunnen jullie referenties geven van vergelijkbare zorginstellingen?

6. Veelgemaakte fouten

Fout 1: Te laat beginnen met de transitie

De deadline voor NEN 7510:2024 implementatie in je ISMS is december 2025. Certificering moet voor 20 februari 2027 [3]. Veel zorginstellingen wachten te lang en komen in tijdnood. Begin nu.

Fout 2: Informatiebeveiliging als IT-project zien

NEN 7510 gaat niet alleen over techniek, maar ook over processen, beleid en gedrag. Als het management niet betrokken is en het als een IT-project wordt gezien, mist het draagvlak en wordt het een papieren exercitie.

Fout 3: Copy-paste documentatie

Template-beleid dat niet aansluit op je daadwerkelijke werkwijze wordt bij de audit direct doorzien. Zorg dat documentatie de werkelijkheid beschrijft, niet een wenssituatie.

Fout 4: Risicoanalyse te oppervlakkig uitvoeren

De risicoanalyse is het fundament van je ISMS. Een oppervlakkige analyse leidt tot irrelevante maatregelen. Besteed hier voldoende tijd en betrek de juiste mensen.

Fout 5: Na certificering achterover leunen

Certificering is het begin, niet het einde. Zonder continue verbetering (de Check-Act fase van PDCA) vervalt je certificaat bij de surveillance-audit.

7. NIS2 en regelgeving

De zorg is onder de Cyberbeveiligingswet (NIS2) aangemerkt als essentieel sector [6]. Dit betekent strenge verplichtingen met boetes tot EUR 10 miljoen. NEN 7510:2024 is bewust geharmoniseerd met de NIS2-vereisten, zodat zorginstellingen met NEN 7510 certificering een groot deel van de NIS2-compliance al afdekken.

8. NEN 7510 vs ISO 27001

KENMERK	NEN 7510	ISO 27001
Doelgroep	Zorgsector specifiek	Alle organisaties
Basis	ISO 27001 + zorgspecifieke aanvullingen	Generiek framework
Wettelijke basis	IGJ handhaving in de zorg	Geen wettelijke verplichting
Aanvullende normen	NEN 7512 (uitwisseling), NEN 7513 (logging)	Geen
Versie 2024	Geharmoniseerd met ISO 27001:2022	ISO 27001:2022

TIP

Op certificeerwijzer.nl vind je een overzicht van certificerende instellingen die NEN 7510 audits uitvoeren.

9. Trends 2025--2026

Transitie naar NEN 7510:2024

Alle certificaathouders moeten voor februari 2027 over naar de nieuwe versie. Dit creert een piek in de vraag naar implementatiebegeleiding en audits [3].

NIS2 integratie

NEN 7510:2024 is bewust afgestemd op de Cyberbeveiligingswet-vereisten. Zorginstellingen die NEN 7510 implementeren, werken tegelijkertijd aan NIS2 compliance.

Digitale dreigingen in de zorg nemen toe

Ransomware en datadiefstal in de zorgsector stijgen. Het NCSC waarschuwt voor toenemende en complexere dreigingen [7].

10. Aan de slag

Begin vandaag met je NEN 7510 implementatie.

1 **Check je huidige situatie**

Heb je al een informatiebeveiligingsbeleid? Een risicoanalyse? Begin met een nulmeting om te weten waar je staat.

2 **Kies een begeleider**

Vergelijk minimaal 3 implementatiebegeleiders op ervaring, prijs en aanpak. Let op zorgspecifieke ervaring.

3 **Plan het traject**

Reken op 12-18 maanden voor volledige implementatie. Begin nu om de transitiedeadline te halen.

Bronnenlijst

[1] **RisGuard** -- NEN 7510 certificering eisen audit en kosten -- risguard.com/nen-7510-certificering/

[2] **BMGRIP** -- Wat kost een NEN 7510 certificering -- bmgrip.nl/wat-kost-een-nen-7510-certificering/

[3] **Cuccibu** -- Herziening NEN 7510 overgangstermijn -- cuccibu.com/blogs/herziening-nen-7510-wat-is-de-overgangstermijn/

[4] **NEN** -- Certificering en register NEN 7510 -- nen.nl/certificatie-en-keurmerken-nen-7510

[5] **Apex Security** -- Kosten cyberincident MKB -- apexsecurity.nl/en/siem-voor-het-mkb-professionele-beveiliging-zonder-enterpriseprijskaartje/

[6] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2) -- digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[7] **NCSC** -- Cybersecuritybeeld Nederland 2025 -- ncsc.nl/actueel/nieuws/2025/11/26/cybersecuritybeeld-2025

[8] **IGJ** -- Vragen over NEN 7510 -- igj.nl/onderwerpen/ehealth/vraag-en-antwoord/vragen-over-nen-7510

[9] **Verizon** -- 2025 Data Breach Investigations Report -- verizon.com/business/resources/reports/dbir/

[10] **NEN** -- Kosteloze Risicotool informatiebeveiliging zorg -- nen.nl/nieuws/actueel/nen-lanceert-kosteloze-risicotool-voor-informatiebeveiliging-in-de-zorg/

[11] **CertificeringsAdvies** -- NEN 7510 voordelen -- certificeringsadvies.nl/wat-is-nen-7510-en-wat-zijn-de-voordelen/

[12] **IBM** -- Cost of a Data Breach 2025 -- ibm.com/reports/data-breach

[13] **DNV** -- NEN 7510:2024 audits -- dnv.nl/nieuws/2025/nen-7510-2024-vanaf-nu-kunnen-audits-worden-uitgevoerd/

[14] **BMGRIP** -- Wijzigingen NEN 7510 -- bmgrip.nl/blogs/dit-zijn-de-vier-belangrijkste-wijzigingen-in-de-nen-7510/

[15] **Diks Process Support** -- Transitie NEN 7510:2024 -- diksprocesssupport.nl/blog/transitie-nen-75102024-wat-verandert-er-en-hoe-pak-je-het-aan/