GIDS

De complete gids voor de NEN 7510 externe audit

Kosten, auditproces, certificerende instellingen, wettelijke eisen, NIS2-verband en zorgspecifieke valkuilen. Met actuele Nederlandse marktdata.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg. Naleving is wettelijk verplicht. Certificering is het sterkste bewijs dat je voldoet.

400+
NEN 7510-gecertificeerde organisaties in het NEN-register
NEN [1]

~50.000
Zorgaanbieders in Nederland -- minder dan 1% is gecertificeerd
CBS / NEN [1]

EUR 5K--15K
Kosten initiële certificeringsaudit voor kleine tot middelgrote zorginstellingen
RisGuard / BMgrip [2][3]

3 jaar
Geldigheid van een NEN 7510 certificaat, met jaarlijkse surveillance
NEN [1]

7
RvA-geaccrediteerde certificerende instellingen voor NEN 7510
NEN [1]

Feb 2027
Deadline transitie naar NEN 7510:2024 voor alle gecertificeerde organisaties
NEN [1]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- ook voor grotere zorgaanbieders
Digitale Overheid [4]

Verplicht
Naleving van NEN 7510 is wettelijk verplicht voor alle zorgaanbieders (Wabvpz)
IGJ [5]

1. Wat is een NEN 7510 externe audit?

Bij een NEN 7510 externe audit beoordeelt een onafhankelijke, geaccrediteerde certificerende instelling of jouw informatiebeveiliging voldoet aan de NEN 7510 norm -- de Nederlandse standaard voor informatiebeveiliging in de zorg.

NEN 7510 is gebaseerd op ISO 27001 maar bevat zorgspecifieke aanvullingen. De norm richt zich op het beschermen van persoonlijke gezondheidsinformatie, zoals patiëntgegevens, medische dossiers en zorginformatie [1].

Naleving van NEN 7510 is wettelijk verplicht voor alle zorgaanbieders. Certificering is niet verplicht, maar het is het sterkste bewijs van naleving richting de Inspectie Gezondheidszorg en Jeugd (IGJ) [5].

> **NEN 7510 = ISO 27001 + zorgspecifiek.** De norm is gebaseerd op de internationale ISO 27001/27002 standaarden plus de zorgspecifieke ISO 27799. Als je al ISO 27001 gecertificeerd bent, is de stap naar NEN 7510 relatief klein [6].

VOOR WIE IS NEN 7510?

- Ziekenhuizen en specialistische klinieken
- Huisartsenpraktijken en gezondheidscentra
- GGZ-instellingen
- VVT-instellingen (verpleging, verzorging, thuiszorg)
- Apothekers en apotheekketen
- Diagnostische centra en laboratoria
- ICT-leveranciers aan de zorg (EPD, lab-systemen, portalen)

GERELATEERDE NORMEN

NORM	ONDERWERP
NEN 7510	Informatiebeveiliging in de zorg (managementsysteem + maatregelen)
NEN 7512	Vertrouwensbasis voor gegevensuitwisseling in de zorg
NEN 7513	Logging van toegang tot patiëntgegevens

2. Het auditproces: Stage 1 en Stage 2

Net als bij ISO 27001 bestaat de NEN 7510 certificeringsaudit uit twee fasen. De zorgspecifieke aandachtspunten maken het verschil.

STAGE 1: DOCUMENTATIE-AUDIT

De auditor beoordeelt of jouw ISMS en documentatie voldoen aan NEN 7510:2024. Dit omvat het informatiebeveiligingsbeleid, de risicoanalyse, de Statement of Applicability en de resultaten van de interne audit. Duur: 1--2 dagen [7].

STAGE 2: IMPLEMENTATIE-AUDIT

On-site beoordeling van de implementatie. De auditor voert interviews, controleert technische maatregelen en beoordeelt registraties. Duur: 2--5 dagen [3].

ZORGSPECIFIEKE AANDACHTSPUNTEN BIJ STAGE 2

- Bescherming van patiëntgegevens in EPD-systemen
- Logging van toegang tot medische dossiers (NEN 7513)
- Beveiliging van gegevensuitwisseling tussen zorginstellingen (NEN 7512)
- Netwerksegmentatie: medische systemen gescheiden van kantoornetwerk
- Fysieke beveiliging van medische apparatuur
- Bewustzijn en training van zorgmedewerkers
- Incidentprocedure voor datalekken met patiëntgegevens

MOGELIJKE UITKOMSTEN

UITKOMST	BETEKENIS	ACTIE
Certificaat	Je voldoet aan NEN 7510:2024	Certificaat wordt afgegeven (3 jaar geldig)
Minor non-conformiteiten	Kleine afwijkingen	Corrigerende acties binnen 90 dagen
Major non-conformiteiten	Ernstige tekortkomingen	Her-audit nodig

3. Wat kost het?

De kosten variëren sterk per type zorginstelling. Een kleine praktijk betaalt aanzienlijk minder dan een ziekenhuis.

KOSTEN INITIËLE CERTIFICERINGSAUDIT

TYPE ZORGINSTELLING	STAGE 1 + STAGE 2
Kleine zorginstelling (huisarts, fysio, ZZP)	EUR 5.000 -- EUR 12.000
Middelgrote zorginstelling (kliniek, GGZ)	EUR 8.000 -- EUR 15.000
Grote zorginstelling (ziekenhuis, VVT)	EUR 12.000 -- EUR 25.000+
ICT-leverancier aan de zorg	EUR 6.000 -- EUR 15.000

Bron: RisGuard [2], BMgrip [3], CertificeringsAdvies NL [8]

JAARLIJKSE KOSTEN NA CERTIFICERING

KOSTENPOST	BEDRAG	FREQUENTIE
Surveillance-audit	EUR 2.000 -- EUR 8.000	Jaarlijks (jaar 2 en 3)
Hercertificering	EUR 5.000 -- EUR 20.000	Elke 3 jaar
ISMS-onderhoud (intern)	EUR 3.000 -- EUR 15.000	Jaarlijks

TOTALE KOSTEN EERSTE 3 JAAR (INDICATIEF)

TYPE	JAAR 1	JAAR 2	JAAR 3	TOTAAL
Kleine instelling	EUR 5.000--12.000	EUR 2.000--4.000	EUR 2.000--4.000	EUR 9.000--20.000
Middelgroot	EUR 8.000--15.000	EUR 3.000--8.000	EUR 3.000--8.000	EUR 14.000--31.000
Groot	EUR 12.000--25.000	EUR 5.000--15.000	EUR 5.000--15.000	EUR 22.000--55.000

Kostenbesparend: Organisaties die al ISO 27001 gecertificeerd zijn, kunnen 30--40% besparen door een combinatie-audit (ISO 27001 + NEN 7510). De overlap is groot [6].

4. De certificatiecyclus

Een NEN 7510 certificaat is 3 jaar geldig. In die periode doorloop je dezelfde cyclus als bij ISO 27001.

1 **Jaar 1: Certificeringsaudit**

STAGE 1 + STAGE 2

Volledige beoordeling van je ISMS tegen NEN 7510:2024.

2 **Jaar 2: Surveillance-audit**

1--2 DAGEN

Steekproefsgewijze controle. Focus op wijzigingen en verbeteracties.

3 **Jaar 3: Surveillance-audit**

1--2 DAGEN

Laatste controle voor hercertificering.

4 **Jaar 4: Hercertificeringsaudit**

VOLLEDIGE HERBEOORDELING

Stage 1 en Stage 2 gecombineerd. Beoordeling van de volledige certificatieperiode.

NEN 7510:2024 TRANSITIE

De nieuwe versie van NEN 7510 is gepubliceerd in december 2024. Alle gecertificeerde organisaties moeten voor 20 februari 2027 overstappen naar NEN 7510:2024. De nieuwe versie bevat een expliciete mapping naar NIS2-vereisten [1].

5. Certificerende instellingen kiezen

Er zijn 7 RvA-geaccrediteerde CI's voor NEN 7510 in Nederland. Kies een CI met ervaring in jouw type zorginstelling.

GEACCREDITEERDE CI'S VOOR NEN 7510

CERTIFICERENDE INSTELLING	BIJZONDERHEDEN
Brand Compliance B.V.	Nederlands, ook ISO 27001
BSI Group Nederland B.V.	Internationaal, ook ISO 27001
DEKRA Certification B.V.	Internationaal, breed portfolio
DNV Business Assurance B.V.	Internationaal, breed portfolio
Kiwa Nederland B.V.	Nederlands, breed portfolio
Noordbeek Certification B.V.	Nederlands, gespecialiseerd
TUV NORD	Internationaal, cluster Z accreditatie

Bron: NEN [1]

WAAROM RVA-ACCREDITATIE ESSENTIEEL IS

Certificaten van niet-geaccrediteerde CI's worden niet erkend door de IGJ. NEN houdt een openbaar register bij van alle NEN 7510-gecertificeerde organisaties -- alleen certificaten van RvA-geaccrediteerde CI's worden opgenomen [1].

TIP

Op certificeerwijzer.nl vind je een actueel overzicht van geaccrediteerde CI's die NEN 7510 audits uitvoeren. Vergelijk op ervaring met jouw type zorginstelling, tarieven en combinatiemogelijkheden met ISO 27001.

6. Wettelijk kader: wat is verplicht?

De juridische basis voor NEN 7510 is stevig. Naleving is verplicht. Certificering is het sterkste -- maar niet het enige -- bewijs.

NALEVING IS VERPLICHT

Sinds 2008 zijn zorgaanbieders wettelijk verplicht om NEN 7510 na te leven. De juridische basis is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). Dit geldt voor alle zorgaanbieders die vallen onder de Wkkgz en persoonsgegevens van patiënten verwerken [9].

CERTIFICERING IS NIET VERPLICHT

Certificering is een middel om naleving aan te tonen, maar niet het enige. Alternatieven zijn een onafhankelijke audit of zelfbeoordeling. Certificering biedt echter het sterkste bewijs richting de IGJ [5].

GERELATEERDE WET- EN REGELGEVING

WET/NORM	VERBAND
Wabvpz	Juridische basis voor NEN 7510-verplichting
Wkkgz	Bepaalt welke zorgaanbieders onder NEN 7510 vallen
AVG / GDPR	Privacybescherming -- complementair aan NEN 7510
Wegiz	Wet elektronische gegevensuitwisseling in de zorg
Cyberbeveiligingswet (NIS2)	Aanvullende eisen voor grotere zorgaanbieders

IGJ-TOEZICHT

De Inspectie Gezondheidszorg en Jeugd (IGJ) houdt toezicht op informatiebeveiliging in de zorg. Bij inspecties let de IGJ op naleving van NEN 7510, NEN 7512 (gegevensuitwisseling) en NEN 7513 (logging). Een certificaat versterkt je positie bij zo'n inspectie [5].

7. Veelgemaakte fouten

Deze zorgspecifieke valkuilen zien auditors regelmatig. Voorkom ze en vergroot je slagingskans.

1 Te veel focus op techniek, te weinig op mensen

Informatiebeveiliging is niet alleen een IT-probleem. Medewerkers die per ongeluk patiëntgegevens delen zijn een groter risico dan een technische kwetsbaarheid [3].

2 Gebrek aan management commitment

"Informatiebeveiliging is toch van IT?" Zonder bestuurlijke betrokkenheid faalt het traject. De directie moet aantoonbaar betrokken zijn [3].

3 Onvolledige asset-inventaris

Systemen, applicaties, EPD-koppelingen en lab-systemen vergeten. Auditors verwachten een compleet overzicht van alle informatiedragers [10].

4 Logging niet op orde (NEN 7513)

Wie heeft wanneer welk patiëntdossier ingezien? Logging is wettelijk verplicht en een veelvoorkomend auditpunt [1].

5 Onvolledige netwerksegmentatie

Medische systemen niet gescheiden van het kantoornetwerk. Dit is een van de meest voorkomende technische bevindingen [11].

6 Externe koppelingen vergeten

EPD-koppelingen, lab-systemen en patiëntportalen worden vaak niet in de scope opgenomen. Auditors verwachten dat alle gegevensstromen in kaart zijn [10].

7 Implementatie puur uit verplichting

"We moeten van de IGJ" leidt tot een ISMS dat niet wordt onderhouden. Certificering heeft alleen waarde als het systeem leeft [3].

8. NIS2 en de Cyberbeveiligingswet

De Cyberbeveiligingswet (NIS2) raakt ook de zorgsector. NEN 7510:2024 maakt de koppeling expliciet.

WANNEER VAL JE ALS ZORGINSTELLING ONDER NIS2?

Zorgaanbieders vallen onder de Cyberbeveiligingswet indien ze minimaal 50 FTE hebben, of een omzet en balanstotaal van meer dan EUR 10 miljoen [4].

NEN 7510 EN NIS2: WAT DEKT HET?

NIS2-EIS	NEN 7510 DEKKING	AANVULLING NODIG?
Risicoanalyse	Volledig	Nee
Incidentmanagement	Deels	Ja -- meldplicht 24--72 uur
Ketenbeveiliging	Deels	Ja -- uitgebreidere analyse
Registratieplicht	Nee	Ja
Bestuurlijke aansprakelijkheid	Nee	Ja

> **NEN 7510:2024 bevat een expliciete mapping naar NIS2.** De nieuwe versie geeft per onderdeel aan hoe NIS2 zich verhoudt tot de NEN 7510 norm. Dit maakt het eenvoudiger om gaps te identificeren en aan te vullen [1].

9. Verschil met ISO 27001 en andere normen

NEN 7510 is geen alternatief voor ISO 27001 -- het is een zorgspecifieke uitbreiding erop.

NEN 7510 VS. ISO 27001

ASPECT	NEN 7510	ISO 27001
Scope	Zorgsector en gezondheidsinformatie	Alle sectoren
Basis	ISO 27001 + ISO 27799	Internationaal framework
Wettelijk verplicht	Ja (Wabvpz)	Nee
Toezichthouder	IGJ	Geen specifiek toezicht
Extra eisen	NEN 7512, NEN 7513	--
Register	Openbaar NEN-register	Geen centraal register
Erkenning	Nationaal (Nederland)	Internationaal

Bron: Brand Compliance [6], Fendix [12]

CERTIFICERING VS. ZELFBEOORDELING

ASPECT	CERTIFICERING	ZELFBEOORDELING
Kosten	EUR 5.000 -- EUR 25.000+	Intern
Objectiviteit	Onafhankelijk	Risico op bias
IGJ-erkenning	Sterkste bewijs	Zwakker
NEN-register	Opname in register	Niet

10. Volgende stappen

Klaar om een NEN 7510 externe audit aan te vragen? Volg dit stappenplan.

1 **Bepaal je startpositie**

Heb je al ISO 27001? Dan is de stap naar NEN 7510 kleiner (delta-audit). Zonder ISO 27001 start je met een gap-analyse tegen NEN 7510:2024.

2 **Breng je informatie-assets in kaart**

Alle systemen, EPD-koppelingen, lab-systemen, patiëntportalen en leveranciers. Vergeet de externe koppelingen niet.

3 **Vergelijk certificerende instellingen**

Vraag minimaal 3 offertes aan bij RvA-geaccrediteerde CI's met ervaring in jouw type zorginstelling. Gebruik certificeerwijzer.nl voor een overzicht.

4 **Zorg voor logging (NEN 7513)**

Logging van toegang tot patiëntgegevens is wettelijk verplicht en een veelvoorkomend auditpunt. Zorg dat dit op orde is.

5 **Plan de audit**

Zorg dat je ISMS minimaal 3 maanden operationeel is en dat je een interne audit en management review hebt uitgevoerd.

HULP NODIG BIJ HET KIEZEN?

Op ibgids.nl/word-gematcht vind je onafhankelijk advies en kun je je laten matchen met geschikte aanbieders voor een NEN 7510 externe audit.

Bronnenlijst

[1] **NEN** -- Informatiebeveiliging in de zorg / Certificering en register NEN 7510 (nen.nl)

[2] **RisGuard** -- NEN 7510 certificering: eisen, audit en kosten (risguard.com)

[3] **BMgrip** -- Wat kost een NEN 7510-certificering (bmgrip.nl)

[4] **Digitale Overheid / Datavoorgezondheid** -- Cyberbeveiligingswet (digitaleoverheid.nl)

[5] **IGJ** -- Vragen over NEN 7510 (igj.nl)

[6] **Brand Compliance** -- Verschillen ISO 27001 en NEN 7510 (brandcompliance.com)

[7] **TUV NORD** -- NEN 7510 certificering (tuv.nl)

[8] **CertificeringsAdvies NL** -- Kosten NEN 7510 (certificeringsadvies.nl)

[9] **Diks Process Support** -- NEN 7510 verplicht: wettelijke eisen (diksprocesssupport.nl)

[10] **DigiTrust** -- Hoe identificeer je informatie-assets voor NEN 7510 (digitrust.nl)

[11] **DigiTrust** -- Welke network security maatregelen vereist NEN 7510 (digitrust.nl)

[12] **Fendix** -- ISO 27001 vs NEN 7510 verschillen (fendix.nl)