GRATIS E-BOOK

NEN 7510 - Wat de zorg écht moet regelen

Begrijpelijke informatiebeveiliging voor zorgorganisaties, zonder jargon

Een uitgave van

Leasa IT

leasa-it.nl

> **Voor wie is dit e-book?**

> Voor bestuurders, kwaliteitsfunctionarissen, IT-/securityverantwoordelijken en compliance-medewerkers in de zorg die weten dat NEN 7510 erbij hoort, maar zoeken naar overzicht: wat houdt het in, geldt het voor ons, en waar beginnen we? Geen normtaal, wel concrete antwoorden.

Voorwoord - waarom NEN 7510, en waarom nu

Patiëntgegevens zijn het meest gevoelige dat een organisatie kan beheren. Een datalek in de zorg is geen gewoon incident. Het raakt vertrouwen, veiligheid en soms direct het welzijn van mensen. Daarom is informatiebeveiliging in de zorg geen vrije keuze, maar een norm: **NEN 7510**.

En de lat ligt hoger dan ooit. Toezichthouders kijken strenger mee, opdrachtgevers en verzekeraars stellen eisen, en met de komst van **NIS2** komt er wetgeving overheen die ook de zorg raakt. Stilstaan is geen optie meer. Los daarvan is NEN 7510 voor zorgaanbieders wettelijk verplicht, ook buiten de **Cyberbeveiligingswet (CBW)**: het Besluit elektronische gegevensverwerking door zorgaanbieders schrijft het voor.

De grootste misvatting? Dat NEN 7510 "iets voor de IT-leverancier" is. Dat is het niet. NEN 7510 gaat over je **hele organisatie**: beleid, mensen, processen én techniek. Het is een bestuurs- en kwaliteitsvraagstuk.

In dit e-book leggen we in begrijpelijke taal uit wat NEN 7510 van je vraagt, of het op jouw organisatie van toepassing is, hoe het samenhangt met NIS2, en welke stappen je concreet kunt zetten.

> **Disclaimer:** dit e-book is bedoeld als praktische introductie en vormt geen juridisch advies. Normen en wetgeving kunnen wijzigen. Laat je specifieke situatie altijd toetsen door een deskundige.

---

1. NEN 7510 in het kort

NEN 7510 is de Nederlandse norm voor informatiebeveiliging in de zorg. De actuele versie is **NEN 7510-1:2024** (december 2024), die de oude versie uit 2017 vervangt. De norm vertaalt de internationale standaarden voor informatiebeveiliging - **ISO/IEC 27001, ISO/IEC 27002 en ISO 27799** - naar de specifieke eisen van de zorg.

De kern in drie zinnen:

1. NEN 7510 borgt de **beschikbaarheid, integriteit en vertrouwelijkheid** van patiënt- en zorggegevens.
2. NEN 7510 vraagt om een **managementsysteem** (ISMS) - structureel beleid, niet een eenmalige actie.
3. NEN 7510 is in de zorg wettelijk **verplicht** en ook **certificeerbaar**.

NEN 7510 bestaat uit twee delen:

- **NEN 7510-1**: de eisen aan het **managementsysteem** (het ISMS), met een normatieve bijlage met zorgspecifieke beheersmaatregelen.
- **NEN 7510-2**: de **beheersmaatregelen** zelf, met implementatierichtlijnen, gebaseerd op ISO/IEC 27002 en de internationale zorgnorm ISO 27799.

Gerelateerde normen vullen dit aan: **NEN 7512** (veilige gegevensuitwisseling tussen zorgpartijen), **NEN 7513** (loggen van inzage in cliëntdossiers) en **NTA 7516** (veilige e-mail met patiëntgegevens).

Aansluiting op andere normen. NEN 7510-1:2024 volgt de geharmoniseerde structuur (Harmonized Structure) voor managementsysteemnormen. Praktisch voordeel: je kunt één **geïntegreerd** managementsysteem opzetten dat tegelijk voldoet aan meerdere normen (bijvoorbeeld ISO 27001 én NEN 7510). Eén keer goed inrichten, meerdere normen tevreden.

Een doorlopend proces. Het ISMS draait continu: plan do check act (PDCA). Compliance is dus geen project met een einddatum, maar een cyclus.

---

2. Geldt NEN 7510 voor mijn organisatie?

De vuistregel is simpel: **verwerk je persoonlijke gezondheidsgegevens, dan is NEN 7510 jouw norm.** Grootte speelt hierbij geen rol. Dat geldt voor een breed scala aan organisaties:

- Ziekenhuizen, klinieken en GGZ-instellingen
- Huisartsen, tandartsen, fysiotherapeuten en andere praktijken
- Thuiszorg, wijkverpleging en ouderenzorg
- Zorgnetwerken en samenwerkingsverbanden
- Leveranciers van zorg-ICT en verwerkers van zorgdata

Wettelijk verplicht en getoetst. Het Besluit elektronische gegevensverwerking door zorgaanbieders (art. 3) verplicht zorgaanbieders om volgens NEN 7510 te werken. Naleving wordt gecontroleerd:

- De **Autoriteit Persoonsgegevens (AP)** beschouwt NEN 7510 als invulling van de 'passende technische en organisatorische maatregelen' zoals vereist onder de **AVG (art. 32).**
- De **Inspectie Gezondheidszorg en Jeugd (IGJ)** hanteert NEN 7510 als toetsingskader om vast te stellen of een zorgaanbieder beschikt over een aantoonbaar werkend informatiebeveiligingsmanagementsysteem.
- **Opdrachtgevers, zorgverzekeraars en ketenpartners** stellen NEN 7510 of aantoonbare informatiebeveiliging conform deze norm steeds vaker als contractuele voorwaarde voor samenwerking.

Je kunt je organisatie ook officieel **laten certificeren** tegen NEN 7510-1, via een geaccrediteerd certificatieschema dat onder toezicht staat van de Raad voor Accreditatie.

> **Let op de keten.** Werk je samen met andere zorgaanbieders of lever je diensten aan de zorg? Dan zullen je partners aantoonbare beveiliging van jóú verwachten. NEN 7510 is steeds vaker een toegangsbewijs om mee te mogen doen.

---

3. Wat eist NEN 7510 concreet?

NEN 7510 vraagt om een managementsysteem met een aantal vaste bouwstenen. In gewone taal:

- **Risicomanagement**: ken de risico's rond je patiëntdata en neem passende maatregelen.
- **Beleid & governance**: vastgelegd informatiebeveiligingsbeleid, met de directie als eindverantwoordelijke.
- **Toegangsbeheer**: wie mag bij welke dossiers? Werk volgens need-to-know en zet multifactor-authenticatie (MFA) in.
- **Logging & controleerbaarheid**: leg vast wie wanneer welk dossier inzag (sluit aan op NEN 7513).
- **Bewustwording & training**: medewerkers herkennen risico's zoals phishing en het verkeerd delen van gegevens.
- **Leveranciers & ketenpartners**: maak afspraken over beveiliging, inclusief verwerkersovereenkomsten.
- **Continuïteit**: back-ups, herstelplannen en een calamiteitenplan voor als het misgaat.
- **Incidentbeheer**: incidenten detecteren, melden, oplossen en ervan leren.
- **Aantoonbaarheid**: documentatie, interne audits en continue verbetering (de PDCA-cyclus).

Kort samengevat: **techniek, processen én mensen** alle drie, structureel geborgd.

---

4. NEN 7510 én NIS2 - de dubbele lat in de zorg

Hier komt een belangrijk punt. De zorg is een sector die ook onder **NIS2** valt; de Europese cyberbeveiligingsrichtlijn, die in Nederland wordt omgezet via de **Cyberbeveiligingswet**. NEN 7510-1:2024 noemt NIS2 zelf al als regelgeving die de zorg raakt. Veel zorgorganisaties krijgen dus met **norm én wet tegelijk** te maken. Goed nieuws: ze overlappen sterk.

	NEN 7510	NIS2
Wat is het?	Nederlandse norm voor de zorg	Europese wet/richtlijn
Verplicht?	Ja, bij wet (Besluit EGZ)	Ja, bij wet (in scope)
Focus	Managementsysteem voor zorgdata	Wettelijke plichten + meldplicht
Meldplicht aan toezichthouder?	Beperkt	Ja (24u / 72u / 1 maand)
Bestuursaansprakelijkheid?	Verantwoordelijkheid directie/ bestuur	Ja, expliciet en persoonlijk

Wat moet je dubbel doen? Eigenlijk weinig. Een goed ingericht NEN 7510-managementsysteem dekt een groot deel van wat NIS2 vraagt. NIS2 voegt vooral wettelijke verplichtingen toe: een **meldplicht met harde termijnen**, een **registratieplicht** en **persoonlijke aansprakelijkheid** voor directie/bestuurders.

De slimme aanpak: richt het **één keer goed** in, en voldoe aan beide. (In ons aparte NIS2-e-book gaan we dieper in op de wettelijke kant, handig als aanvulling.)

---

5. De rol van bestuur en directie

NEN 7510 legt de eindverantwoordelijkheid expliciet bij de **directie/bestuur**. Dat betekent concreet:

- Directie/bestuur **stelt het beleid vast** en maakt middelen vrij.
- Directie/bestuur **houdt toezicht** op de uitvoering en de resultaten.
- Informatiebeveiliging wordt onderdeel van de **kwaliteits- en risicocyclus** van de organisatie.

En misschien wel het belangrijkst: Directie/bestuur geeft het **goede voorbeeld**. Veilig werken is een cultuur van de baliemedewerker tot de specialist. Als de top het serieus neemt, volgt de rest.

---

6. De 10 meest gemaakte fouten

1. **NEN 7510 zien als "IT-feestje"** in plaats van een organisatiebrede verantwoordelijkheid.
2. **Beleid op papier**, maar niet geleefd in de dagelijkse praktijk.
3. **Toegangsrechten te ruim** iedereen kan bij alle dossiers.
4. **Geen logging op dossierinzage** (NEN 7513), waardoor je niet kunt aantonen wie wat zag.
5. **Medewerkers niet trainen** terwijl de mens de grootste kwetsbaarheid is.
6. **Leveranciers en ketenpartners niet contractueel borgen.**
7. **Back-up nooit getest** bij ransomware sta je dan alsnog stil.
8. **Eenmalig certificeren** en daarna stilstaan, zonder verbetercyclus.
9. **NEN 7510 en NIS2 los aanpakken** in plaats van slim combineren.
10. **Tijd en capaciteit onderschatten** informatiebeveiliging erbij doen, naast de zorg.

---

7. Praktische checklist - ben ik audit-klaar?

Loop deze lijst door. Elke "nee" is een actiepunt.

Beleid & governance

- ☐ Er is een actueel, vastgesteld informatiebeveiligingsbeleid.
- ☐ De directie is betrokken en eindverantwoordelijk.
- ☐ Informatiebeveiliging zit in de kwaliteits-/risicocyclus.

Maatregelen

- ☐ Er is een actuele risicoanalyse op patiënt-/zorgdata.
- ☐ Toegangsrechten zijn ingericht op need-to-know, met MFA.
- ☐ Dossierinzage wordt gelogd (NEN 7513).

- ☐ Back-up- en herstelplannen zijn aanwezig én getest.
- ☐ Medewerkers krijgen periodiek awareness-/securitytraining.
- ☐ Afspraken met leveranciers/ketenpartners zijn vastgelegd.

Aantoonbaarheid

- ☐ Maatregelen zijn gedocumenteerd en actueel.
- ☐ Er worden interne audits en verbetercyclus (PDCA) uitgevoerd.
- ☐ Ik kan bij een audit aantonen dat beleid ook echt wordt nageleefd.

Vink je hier niet alles aan? Dan is er werk aan de winkel en dat is precies waar het volgende hoofdstuk over gaat.

---

8. Van weten naar aantoonbaar voldoen

Na het lezen van dit e-book begrijp je NEN 7510. Maar begrijpen is iets anders dan **aantoonbaar voldoen**. Het verschil:

- **Weten** is een checklist doorlopen.
- **Doen** is beleid schrijven, techniek inrichten, toegang en logging regelen, leveranciers contracteren, medewerkers en bestuur trainen, een incidentproces opzetten en dat allemaal documenteren zodat het een audit doorstaat. En het vervolgens blijven onderhouden.

Voor de meeste zorgorganisaties is dat maanden werk, met kennis en capaciteit die er naast de zorg vaak niet volledig is. En juist daar zit het risico: de eisen worden strenger, de verantwoordelijkheid ligt bij de directie, en half werk telt bij een audit niet.

Hoe Leasa IT hierbij helpt. Wij leveren werkplekken als dienst waarin beveiliging en compliance van begin af aan zijn ingebouwd die voldoen aan **NEN 7510 en NIS2**. Daarbij ondersteunen we met:

- **Gap- en projecttooling** om helder te krijgen waar je staat en wat er nog moet gebeuren.
- **Bestuurderstrainingen** zodat de directie zijn rol kan pakken.
- **Awareness-/securitytrainingen** voor je medewerkers, de menselijke firewall.
- **Beheer, monitoring en updates** zodat compliance geborgd blijft, niet eenmalig is.

Zo verschuift de last van "alles zelf uitzoeken en bijhouden" naar "het is geregeld, en aantoonbaar" zodat jij je kunt richten op je patiënten.

---

9. De volgende stap

NEN 7510 is geen reden voor stress, maar wél voor actie. De zorgorganisaties die nu hun beveiliging op orde brengen, zijn straks audit-klaar zonder gedoe en stralen vertrouwen uit naar patiënten, partners en toezichthouders.

Wil je weten waar jouw organisatie staat?

Plan een **gratis check van 10 minuten** met Leasa IT. We kijken samen waar je staat ten opzichte van NEN 7510 (en NIS2) en wat de meest logische volgende stappen zijn. Zonder verplichtingen.

> **Plan je gratis check op leasa-it.nl/contact**

Leasa IT "Veilige, compliant werkplekken zonder gedoe. Van device tot bestuurskamer".