NEN 7510 Informatiegids

CertificeringsAdvies
NEDERLAND
advies, opleiding & outsourcing

In deze whitepaper

Met de toenemende digitalisering, is informatiebeveiliging voor meer en meer organisaties van vitaal belang. De gezondheidszorg heeft, in tegenstelling tot andere branches, te maken met veel persoonlijke gezondheids-gegevens die vertrouwelijk van aard zijn. Informatie-beveiliging staat binnen de zorgsector daarom sterk op de radar. Verder is het natuurlijk zo dat met de komst van de AVG-wet de regels rondom medische gegevens strenger zijn geworden. Medische gegevens gelden als bijzondere persoonsgegevens en genieten daardoor extra bescherming.

Het is dus essentieel dat persoonlijke gezondheidsdata goed beveiligd wordt (opgeslagen) en dat er vertrouwelijk met de gegevens om wordt gegaan. Met een NEN 7510:2017 certificering kun je als organisatie aantoonbaar maken dat je dit goed hebt geborgd. In deze whitepaper vertellen we:

- Wat NEN 7510 precies is;
- Voor wie NEN 7510 verplicht is;
- Wat een NEN 7510 ISMS is;
- Hoe het stappenplan voor NEN 7510 eruitziet;
- Over het verschil tussen NEN 7510 en ISO 27001.

Daarnaast vind je in deze whitepaper een aantal veelgestelde vragen over NEN 7510 met de bijbehorende antwoorden. Zo hopen we je een compleet beeld te geven van de toegevoegde waarde van een NEN 7510 certificering voor jouw organisatie.

Inhoudsopgave

1. Wat is NEN 7510?

NEN 7510 is een Nederlandse ‘specificatie’ van de ISO 27001 norm voor informatiebeveiliging voor de zorgsector. NEN staat voor Nederlands Normalisatie-instituut. Een NEN-norm is daarmee een norm die vooral in gebruik is in Nederland. NEN 7510 biedt zorginstellingen een leidraad voor het formuleren, vastleggen en controleren van de interne informatiebeveiliging. Belangrijk natuurlijk, vanwege de verwerking van gevoelige gegevens.

De NEN 7510 norm is gebaseerd op ISO 27001, maar bij NEN 7510 zijn 33 van de 114 standaard beheersmaatregelen van ISO 27001 uitgebreid met een specifieke ‘vertaling’ naar de zorg. Daarnaast zijn er 3 extra maatregelen specifiek voor de zorg toegevoegd. Om het NEN 7510 certificaat te behalen, moet je als organisatie aantoonbaar maken dat je voldoet aan de eisen uit de norm.

2. Voor wie is NEN 7510 verplicht?

De NEN 7510 norm is specifiek ontwikkeld voor informatie-beveiliging binnen de Nederlandse zorgsector. De norm biedt alle type zorgaanbieders die werkzaam zijn binnen de gezondheids-zorg of organisaties die bij de informatievoorziening betrokken zijn een leidraad voor het formuleren, vastleggen en controleren van de interne informatiebeveiliging. Deze organisaties dienen de juiste IT-beveiligingsprotocollen door te voeren en kritisch te kijken naar de gegevensverzameling en de noodzaak daarvan.

Doordat er in de gezondheidssector veel gevoelige gegevens worden verwerkt heeft NEN 7510 voor zorginstellingen (zieken-huizen, verpleeghuizen, GGZ-instellingen, fysiotherapie-praktijken etc.) een verplichtend karakter. Zorgverleners zijn met het oog op de AVG-wet in het kader van de verwerking van het Burgerservicenummer al verplicht om aan NEN 7510 te voldoen. Ook zijn er binnen de zorgbranche diverse partijen die NEN 7510 eisen als aansluitvoorwaarde, denk bijvoorbeeld aan Vecozo of MedMij. Dat betekent dat de NEN 7510 certificering niet enkel relevant is voor zorgverlenende instanties, maar ook voor toeleveranciers zoals:

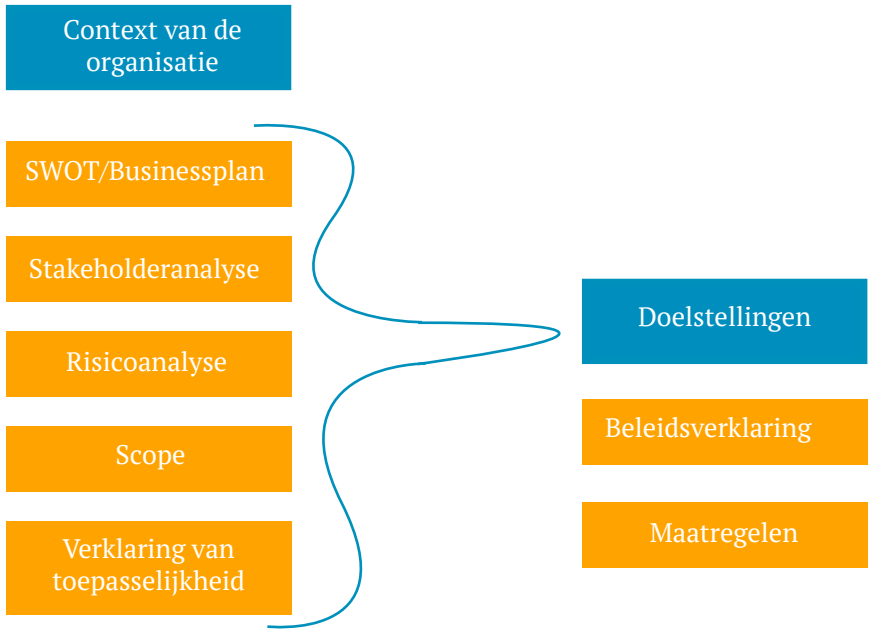
- Leveranciers van zorgapplicaties;
- Tussenpartijen voor zorgadministratie en/of -declaratie;
- Andere verwerkers van persoonlijke gezondheidsinformatie.

NEN 7510 is van toepassing voor organisaties die in aan-raking komen met persoonlijke gezondheidsinformatie. Dit kan binnen de organisatie zelf zijn (zorgverlener), via een interface naar een zorginstelling, danwel door uitbesteding van bepaalde (ICT of andere) processen. Je ziet dan ook dat er van toeleveranciers aan de zorgsector steeds vaker wordt verlangd dat zij het NEN 7510 certificaat behalen.

3. Het NEN 7510 Information Security Management System (ISMS)

Een Information Security Management System (ISMS) is een managementsysteem voor informatiebeveiliging. Bij een managementsysteem wordt vaak gedacht aan een dik en wollig handboek waarin alles wat de organisatie doet dient te worden beschreven. Het gaat bij een NEN 7510 ISMS echter om veel meer dan alleen het uitwerken van beleidsstukken en procedures. Het NEN 7510 Information Security Management System (ISMS) moet helpen bij de bedrijfsvoering van de organisatie en ervoor zorgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gezondheidsinformatie geborgd en verbeterd wordt.

Bij een managementsysteem voor NEN 7510 dient de context van de organisatie in kaart te worden gebracht. Vanuit deze context wordt het informatiebeveiligingsbeleid van de organisatie bepaald en van daaruit worden doelstellingen geformuleerd die de organisatie wil bereiken om de beveiliging van gezondheids informatie beter te borgen. Dat ziet er schematisch gezien als volgt uit:



Als de doelstellingen geformuleerd zijn, gaat de organisatie een GAP-analyse uitvoeren op de beheersmaatregelen. Daarbij wordt in kaart gebracht welke beheersmaatregelen al geïmplementeerd zijn en wat de organisatie nog wil/moet implementeren. Dit gebeurt op basis van de risicoanalyse. Deze GAP-analyse dient als leidraad voor de verdere implementatie van het NEN 7510 ISMS.

Voor meer informatie, lees ook het artikel:

‘NEN 7510 Information Security Management System (ISMS)’

4. Stappenplan voor NEN 7510:2017 certificering

Voordat een organisatie het NEN 7510:2017 certificaat ontvangt, dienen de volgende stappen doorlopen te worden:

Fase	Stap	Activiteit
Fase 1	1	Algemene inventarisatie van de organisatie (werkwijze, beschikbare informatie, infrastructuur etc. + scope bepaling.
	2	Uitvoeren contextanalyse (in kaart brengen van stakeholders en relevante risico's /kansen).
	3	Uitvoeren risicoanalyse o.b.v. de NEN 7510 normelementen (zie o.a. Annex A van de norm).
	4	Opstellen Plan van Aanpak (vaststellen benodigde maatregelen en eisen aan het managementsysteem, afstemmen actieplan).
Fase 2	5	Aanscherpen contextanalyse.
	6	Beleidscyclus: vaststellen proces van bepalen beleid/doelstellingen, vertaling naar organisatie en bewaking hiervan.
	7	Uitvoeren Plan van Aanpak.
	8	Borging en implementatie; gemaakte afspraken en procedures vastleggen in het managementsysteem en implementeren binnen de organisatie.
	9	Interne audit: uitvoeren interne audit ter controle van een effectieve implementatie en ter voorbereiding op de certificeringsaudit.
	10	Certificering: de certificering wordt uitgevoerd door een erkende certificerende instantie.

5. Het verschil tussen NEN 7510 en ISO 27001

De belangrijkste en meest voorkomende certificeringen in Nederland op het gebied van informatiebeveiliging zijn ISO 27001 en NEN 7510. ISO 27001 is de internationale norm voor informatiebeveiliging en biedt een raamwerk voor het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in een organisatie. De norm is toepasbaar binnen alle branches. Maar wanneer kies je nu voor NEN 7510 en wanneer voor ISO 27001?

We hebben het hier over informatiebeveiliging. Het soort informatie is dan ook het belangrijkste criterium als het gaat om een keuze voor ISO 27001 of NEN 7510. Onderscheidend tussen ISO 27001 en NEN 7510 is daarbij de vraag of het gaat om gezondheidsinformatie of niet. Is er géén sprake van gezondheidsgegevens die beveiligd moeten worden, dan is NEN 7510 niet toepasbaar en kies je automatisch voor ISO 27001. Heeft de informatiebeveiliging wel betrekking op gezondheidsinformatie (binnen de organisatie zelf of via een interface naar een zorginstelling, danwel door uitbesteding van bepaalde processen), kies dan altijd voor NEN 7510.

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Er kan soms ook een reden zijn om voor zowel ISO 27001 als NEN 7510 te kiezen. Dat heeft namelijk te maken met het toepassingsgebied (de 'scope') van de certificering. Wanneer je te maken hebt met internationale belanghebbenden m.b.t. de informatie waar je certificering op van toepassing is, dan volstaat alleen een NEN 7510 certificering mogelijk niet. In dat geval loont het om voor ISO 27001 certificering te gaan. Een andere reden om voor beide certificaten te gaan, is als voor jouw organisatie (en jouw stakeholders) naast gezondheidsinformatie ook andersoortige informatie relevant is om aantoonbaar te beveiligen.

Meer informatie? Lees het artikel:

'Kiezen voor ISO 27002 of NEN 7510 of beide? En zijn er alternatieven?'

6. Veelgestelde vragen over NEN 7510

6.1. Wat kost een NEN 7510 certificering?

Het is verstandig om als organisatie het kostenplaatje in kaart te brengen als je NEN 7510 wilt certificeren. Er zit immers verschil in de kosten en de aanpak van de verschillende consultancybureaus en certificerende instanties. Iedere organisatie is echter uniek en heeft unieke risico's die de impact van de informatiebeveiliging bepalen. Een NEN 7510 traject is daarom vaak maatwerk. De impact en kosten kunnen pas bepaald worden na een analyse van de huidige situatie en risico's. Bovendien is de investering in een consultant afhankelijk van de hoeveelheid werk die je wilt uitbesteden en de rol die aan de consultant wordt toebedeeld (coachend / uitvoerend).

Desalniettemin kunnen we bij CertificeringsAdvies Nederland, op basis van onze ruime ervaring op dit gebied, aan de hand van een intake een offerte op maat maken voor jouw organisatie. Zo weet je wat de investering gaat zijn als je aan de slag gaat met de implementatie van de norm.

6.2 . Wat is de doorlooptijd van een NEN 7510 implementatie?

Het is vooraf lastig te zeggen hoelang een dergelijk traject precies duurt. Dit is namelijk o.a. afhankelijk van:

- De huidige stand van zaken binnen de organisatie;
- De aanwezige organisatorische, technische en fysieke beheersmaatregelen;
- De complexiteit van de organisatie;
- De grootte van de organisatie;
- De interne capaciteit en slagkracht van de organisatie.

Wanneer je als organisatie je bedrijfsprocessen helder in kaart hebt, gaat implementatie sneller dan wanneer je vanaf nul moet beginnen. Des te meer er al is en des te minder complex de organisatie in elkaar steekt, des te sneller het NEN 7510 traject doorlopen kan worden.

Wanneer je vervolgens aan wilt tonen dat je de informatie-beveiliging op orde hebt, dan kun je dat ISMS laten toetsen en uiteindelijk laten certificeren door een onafhankelijke, certificerende instantie. Wil je een dergelijke toetsing succesvol doorlopen, dan dien je aan te kunnen tonen dat je voldoende aandacht besteedt aan informatiebeveiliging. Daarvoor moet je minimaal drie maanden volgens het ISMS hebben gewerkt. Dit wordt ook wel de ‘bewijsperiode’ genoemd. Na drie maanden kan een externe auditor namelijk beoordelen of het ISMS in de praktijk functioneert.

Op basis van onze ervaring kunnen we bij CertificeringsAdvies Nederland wel een indicatie geven van de doorlooptijd. Voor een NEN 7510 certificeringstraject wordt een minimale doorlooptijd van 5 tot 6 maanden aangehouden. Bij grotere organisaties kan het zomaar 8 tot 12 maanden duren.

6.3. Zijn er alternatieven voor ISO 27001 en NEN 7510?

Naast de zorgsector zijn er nog enkele sectoren waar een 'sector-specifieke vertaling' van ISO 27001 de gebruikelijke standaard is voor informatiebeveiliging, te weten de Baseline Informatie-beveiliging voor de Overheid (BIO) en de Algemene Beveiligings-eisen voor Defensieopdrachten (ABDO). Indien je je als organisatie in dit 'speelveld' bevindt, zijn deze normen van toepassing. Afgezien van deze nuancering/kanttekening, kunnen we concluderen dat ISO 27001 en NEN 7510 in Nederland als dé standaarden gelden voor informatiebeveiliging.

6.4. Wanneer kies je voor ISAE 3402?

Naast ISO 27001 en NEN 7510 zijn er normen op de markt waar-mee specifieker op bepaalde onderdelen/aspecten van informa-tiebeveiliging binnen je organisatie kan worden ingezoomd. Denk daarbij bijvoorbeeld aan ISAE 3402. Deze norm heeft betrekking op uitbestede processen. Door middel van een ISAE3402 verklaring (type I en/of II) geef je als serviceorganisatie (leverancier) in opdracht van een gebruikersorganisatie (klant) inzicht in de getroffen (informatiebeveiligings)maatregelen waarmee directe en indirecte financiële risico's voor de betreffende gebruikersorganisatie 'in control' zijn. ISAE 3402 is een accountantsonderzoek en -verklaring, waarbij ieder aspect jaarlijks beoordeeld moet worden.

Bij NEN 7510 wordt naast de opzet van het ISMS veel meer gekeken naar het vermogen van de organisatie om zelf afwijkingen te signaleren, deze op te pakken en op deze manier continu te verbeteren. De insteek van een ISAE 3402 verklaring is wezenlijk anders dan die van een NEN 7510/ISO 27001 certificering.

6.5. Wat is de Verklaring van Toepasselijkheid binnen NEN 7510?

Deze verklaring hangt samen met de risicoanalyse. In feite is de Verklaring van Toepasselijkheid een opsomming van het-geen dat van toepassing is voor een bedrijf en geïmplementeerd dient te worden om risico's te mitigeren. De NEN 7510:2017 norm heeft een bijlage (Annex A) die alle beheersmaatregelen omvat. De Verklaring van Toepasselijkheid is een document waarin de organisatie deze beheersmaatregelen van toepassing verklaart of niet. Deze verklaring maakt uiteindelijk integraal onderdeel uit van het NEN 7510 certificaat van de organisatie.

CERTIFICERINGSADVIES NEDERLAND

JOUW PARTNER IN CERTIFICEREN

CertificeringsAdvies NEDERLAND
advies, opleiding & outsourcing

Heb je vragen over de NEN 7510?
Of wil je de informatiebeveiliging in je organisatie naar een hoger niveau tillen? Neem dan contact op met CertificeringsAdvies Nederland.

Deze whitepaper is geschreven door CertificeringsAdvies Nederland. Als Partner In Certificeren helpen wij organisaties met advies, opleiding en outsourcing binnen de thema's Kwaliteit, Arbo en Veiligheid, Milieu en MVO, Informatie-beveiliging en Voedselveiligheid.

CertificeringsAdvies Nederland werkt onder andere voor:

totall-it

CITO

universal
a touch of power