FAQ’s NEN 7510

Vragen over de norm NEN 7510

Sinds december 2017 zijn de nieuwe normen NEN 7510-1:2017 en NEN 7510-2:2017 beschikbaar zijn. Is er een overgangsperiode vastgesteld, en zo ja: hoe lang is deze periode?

De nieuwe NEN 7510:2017 is 7 december jl. gepubliceerd en hiermee is NEN 7510:2011 ingetrokken. Gebruik van NEN 7510:2011 voor certificatiedoeleinden onder accreditatie blijft mogelijk, uiterlijk tot 1 juni 2020.

Beschikt NEN over Engelse versies van NEN 7510, NEN 7512 en NEN 7513?

NEN 7510, NEN 7512 en NEN 7513 zijn Nederlandse normen waarvan geen Engelse versie bestaat. Deze normen gelden ook alleen in Nederland. Echter, met name NEN 7510 is gebaseerd op internationale nomen. NEN 750-1 heeft als equivalent ISO 27001 en NEN 7510-2 combineert ISO 27002 met ISO 27799. Al deze internationale normen zijn in het Engels beschikbaar.

Is er een overzicht beschikbaar van hoe de voorschriften uit NEN 7510:2011 in de nieuwe NEN 7510:2017 terecht zijn gekomen?

Ja, Deel 1 van NEN 7510:2017 bevat een bijlage waarin een gedetailleerde vergelijking van NEN 7510-1:2017 en NEN 7510-2:2017 met NEN 7510:2011 is opgenomen.

Wat is de relatie tussen NEN 7510, NEN 7512 en NEN 7513?

NEN 7510 is een managementsysteemnorm die een kader stelt voor het organiseren en borgen van informatiebeveiliging binnen een zorginstelling of toeleverancier. NEN 7512 (7510-2, 13.2) en NEN 7513 (7510-2, paragraaf 12.4)zijn aanvullingen op (specifieke eisen uit) NEN 7510.

Geldt de nieuwe norm ook voor gemeenten? Gemeenten zijn verantwoordelijk voor WMO en jeugdzorg en hebben met medische gegevens te maken.

Ja, NEN 7510 is ook van toepassing op gemeenten. NEN 7510 richt zich niet alleen op zorginstellingen, maar daarnaast ook op alle andere organisaties die persoonlijke gezondheidsinformatie verwerken. Dus ook op gemeenten indien en voor zover ze persoonlijke gezondheidsinformatie verwerken.

Wat verhouden zich ISO 27001, ISO 27002 en NEN 7510:2017 deel 1 en 2 tot elkaar?

NEN 7510 en ISO 27001 zijn allebei normen, die iets zeggen over hoe organisaties zouden kunnen/moeten omgaan met informatiebeveiliging.

Het verschil tussen NEN 7510 en ISO 27001 is dat NEN 7510 is toegespitst op de zorg. In de zorg is de privacy van cliënten afhankelijk van het handhaven van de vertrouwelijkheid van persoonlijke gezondheidsinformatie. Om deze vertrouwelijkheid te handhaven, moeten er ook maatregelen worden genomen voor het handhaven van de integriteit van gegevens, al was dat alleen maar vanwege het feit dat het mogelijk is de integriteit van toegangsbeveiligingsgegevens, audittrajecten en andere systeemgegevens dusdanig te corrumperen dat schendingen van de vertrouwelijkheid kunnen plaatsvinden en zelfs onopgemerkt kunnen blijven.

Bovendien is de veiligheid van cliënten afhankelijk van het handhaven van de integriteit van persoonlijke gezondheidsinformatie; nalatigheid kan ziekte, letsel of zelfs de dood als gevolg hebben. Een hoog beschikbaarheidsniveau is ook een bijzonder belangrijk kenmerk van zorginformatiesystemen, waar behandelingen vaak tijdkritisch zijn. Het zou zo kunnen zijn dat juist het moment waarop zich rampen voordoen, die zouden kunnen leiden tot uitval van andere, niet-gezondheidsgerelateerde IT-systemen, het moment is waarop de in zorginformatiesystemen vervatte informatie het hardst nodig is.

De in NEN 7510-1 en NEN 7510-2 besproken beheersmaatregelen zijn de beheersmaatregelen waarvan is bepaald dat ze geschikt zijn om de vertrouwelijkheid, integriteit en beschikbaarheid van persoonlijke gezondheidsinformatie in de zorg te beschermen en ervoor te zorgen dat de toegang tot dergelijke informatie gecontroleerd en verantwoord kan worden. Deze beheersmaatregelen helpen fouten in de medische praktijk te voorkomen, die zouden kunnen voortvloeien uit het niet goed handhaven van de integriteit van gezondheidsinformatie. Bovendien dragen ze bij aan het garanderen dat de continuïteit van medische dienstverlening gehandhaafd wordt.

NEN 7510:2017 bestaat uit twee delen. Deel 1 bevat de normatieve voorschriften voor het managementsysteem volgens ISO 27001. Deel 2 vormt de Nederlandse weergave van de Europese en mondiale normen ISO 27002 én ISO 27799. Meer dan bij de 2011-versie, is aangesloten bij indeling, structuur en teksten van de internationale normen. Zo zijn de, speciaal voor de zorg geschreven, aanvullende beheersmaatregelen uit ISO 27799 vertaald en integraal in de nieuwe NEN 7510 opgenomen.

De nieuwe norm biedt daarmee een integraal Nederlandstalig kader voor informatiebeveiliging, toegespitst op de Nederlandse situatie in de zorg. Ook is de vernieuwde High Level Structure nu geheel in de norm opgenomen. NEN 7510 is hierdoor compatibel met andere managementsysteemnormen die de HLS volgen.

Richt NEN 7510 zich ook op softwareontwikkelaars die zich focussen op zorginstellingen/ondernemingen?

De scope van NEN 7510 richt zich op zorgorganisaties en andere beheerders van persoonlijke gezondheidsinformatie. Bij leveranciers is het relevant te constateren of zij zelf persoonlijke gezondheidsinformatie ‘verwerken’. Meer informatie over wat persoonlijke gezondheidsinformatie is, vindt u op de site van AVG.

NEN 7510 in de praktijk

Hoe bepaalt een zorginstelling in hoeverre NEN 7510 op haar organisatie van toepassing is?

NEN 7510 beschrijft een set maatregelen die organisaties in de gezondheidszorg moeten treffen om via een gecontroleerd proces op adequate wijze met (medische) gegevens om te gaan. De norm is van toepassing op alle organisaties in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces.

Met een nulmeting kunt u bepalen in hoeverre uw organisatie bewust is van informatiebeveiliging en eventueel al voldoet aan de gestelde eisen. Hierna kan uw organisatie op basis van een risicoanalyse vaststellen welke risico's prioriteit moeten hebben en wat de te nemen maatregelen zijn. Het staat de verantwoordelijke vrij om te bepalen hoever deze wil gaan met de invoering en handhaving van de maatregelen en eventueel externe toetsing hierop (certificatie).

Wie is verantwoordelijk voor de informatiebeveiliging in de zorg?

De complexiteit van informatiebeveiliging in de zorgsector blijkt duidelijk uit de veelheid van partijen en disciplines, het netwerk van zorginstellingen en andere belanghebbenden die een rol spelen in het verzamelen, opslaan, verwerken en transporteren van gegevens. Elke organisatie in de zorg heeft haar eigen verantwoordelijkheid voor het beveiligen van patiëntgegevens die onder haar hoede worden vastgelegd.

Gezien het feit dat Google Chrome wordt ingezet in de zorg als browser, en in relatie tot het delen van medische gegevens: In hoeverre is Google Chrome NEN 7510 compliant?

Een bepaalde browser (of enige andere soort applicatie) kan op zichzelf niet ‘NEN 7510 compliant’ zijn. Deze norm richt zich namelijk op organisaties, niet op producten, applicaties of systemen.
Het zijn de zorginstellingen (en andere organisatie die persoonlijke gezondheidsinformatie ‘verwerken’ die moeten voldoen aan NEN 7510. In dit geval dient de organisatie die Google Chrome gebruikt zich ervan te vergewissen dat de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens die met Chrome worden verwerkt gewaarborgd is.

Wat wordt er bedoeld met de begrippen 'Beveiligde' en 'Veilige'. Betreft dit andere technieken?

‘Veilig’ betekent inherent veilig. ‘Beveiligd’ betekent dat het veilig moet worden gemaakt.
Veilig verwijderen is dan bijvoorbeeld het door middel van vertrouwde personen en het toepassen van correcte procedures malversaties tegengaan. Beveiligd verwijderen is dan het gebruik maken van deze personen, procedures etc. op zo’n manier dat die personen de procedures zelf niet kunnen manipuleren, bijvoorbeeld door het toepassen van het vier ogen-principe.

Het gaat dus niet zozeer om verschillende technieken. Zie ook de Engelse tekst van ISO 27002 vertaald naar het Nederlands:
ISO 27002: 8.3.2: Media should be disposed of securely when no longer required, using formal procedures - Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Wat is een geavanceerde elektronische handtekening en is zo'n handtekening wel veilig?

Voor een 'gewone' elektronische handtekening gelden de volgende eisen:

- Ze moet op een unieke wijze aan de ondertekenaar zijn verbonden;
- De ondertekenaar moet kunnen worden geïdentificeerd;
- Ze moet tot stand komen met middelen die de ondertekenaar onder zijn controle kan houden;
- Elke wijziging van de gegevens moet kunnen worden opgespoord.

De geavanceerde elektronische handtekening gaat nog een stap verder. Ze moet zijn gebaseerd op een gekwalificeerd certificaat en zijn gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen, conform de Europese richtlijn 1999/91/EG.

Wanneer ik als zorginstelling (cloud)software gebruik die volledig ISO 27001 gecertificeerd is, voldoe ik dan ook direct aan NEN 7510?

De cloud-oplossing op zichzelf kan niet tegen ISO 27001 en ook niet tegen NEN 7510 gecertificeerd zijn. Deze normen richten zich op organisaties.
De organisatie achter de cloudoplossing is mogelijk gecertificeerd tegen ISO 27001, maar dat betekent zeker niet dat ze daarmee ook tegen NEN 7510 gecertificeerd zijn. Daarvoor mist dan het zorgspecifieke deel.

Is de training 'ISO 27001: INFORMATIEBEVEILIGING IN DE PRAKTIJK / NEN 7510 ….'geschikt voor het verkrijgen van voldoende informatie voor het opzetten van een goed privacybeleid?

In de training wordt op meerdere momenten aandacht besteed aan de vereisten die samenhangen met invoering van de nieuwe privacy wetgeving. Verschillende eisen uit NEN 7510 geven een goede basis voor het implementeren van de AVG. Maar NEN 7510 en privacy zijn niet hetzelfde en een informatiebeveiligingsbeleid conform NEN 7510 kan wel een goede basis vormen voor, maar is niet hetzelfde als een privacybeleid.

In aanvulling op de bestaande trainingen start NEN in de tweede helft van 2018 met trainingen specifiek gericht op het implementeren van AVG met behulp van normen. ISO 27001 zal daar een belangrijk onderdeel van uitmaken.

NEN 7510 in relatie met verplichtingen en wet- en regelgeving

Is het gebruik van NEN 7510 verplicht?

Zowel Wbp als AVG verplichten organisaties te zorgen voor een adequate beveiliging van persoonsgegevens. In art. 32 AVG is vastgesteld dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

Het ontwerpbesluit **Besluit elektronische gegevensverwerking door zorgaanbieders** verwijst dwingend naar NEN 7510, NEN 7512 en NEN 7513. De Nota van toelichting bij dit besluit vermeldt de verplichting om te voldoen aan NEN 7510 en NEN 7512 in het kader van de verwerking van het burgerservicenummer.

De **Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg** (Ook bekend onder de titel: Wet cliëntenrechten bij elektronische verwerking van gegevens) schept aanvullende randvoorwaarden voor het eventuele gebruik van een elektronisch uitwisselingssysteem door zorginstellingen en wijzigt naar een aantal andere wetten. In art. 10 wordt bepaald dat bij ministeriële regeling kan worden bepaald aan welke beveiligingseisen de gegevensverwerking moet voldoen. In de op dat artikel gebaseerde Regeling gebruik burgerservicenummer in de zorg staat in art. 2 dat die gegevensverwerking moet voldoen aan NEN 7510.

Is NEN 7510 ook op een gehandicaptenzorginstelling van toepassing?

Indien uw zorginstelling patiëntgegevens verwerkt, dan moet uw organisatie voor adequate informatiebeveiliging zorgen. NEN 7510 geeft hiertoe een kader. De norm adviseert zorgorganisaties een risico-inventarisatie en -analyse uit te voeren en op basis daarvan maatregelen vast te stellen, in te voeren en te borgen.
Indien uw zorginstelling gebruik maakt van burgerservicenummers, dan moet uw organisatie zich houden aan de AVG. Het beveiligen van persoonsgegevens is op basis van deze wet verplicht.

Als ik aan NEN 7510 voldoe, voldoe ik dan ook aan de AVG?

Nee, er zijn een aantal eisen uit de AVG die afgedekt worden door NEN 7510, maar dit is niet volledig.

In welke mate zijn normen verplicht?

Elk Europese lidstaat heeft een bij wet aangewezen normalisatie-instituut waarvan NEN het aangewezen instituut voor Nederland is. Er bestaan wet- en regelgeving die verwijzen naar normen waarmee deze een verplichtend karakter krijgen, maar normen zijn vrijwillig tot stand gekomen privaatrechtelijke documenten die organisaties niet verplichten tot het gebruik ervan. Met andere woorden, een organisatie kan altijd voor een alternatief kiezen, mits het voldoet aan de minimaal gestelde eisen die in de desbetreffende norm zijn vastgesteld.

Certificatie NEN 7510

Wat houdt certificeren in

Certificeren is het onafhankelijk beoordelen om aan te tonen of aan de eisen uit een norm wordt voldaan. De organisaties die deze toetsing uitvoeren, worden certificerende instellingen genoemd. In normen zijn de eisen vastgelegd waaraan een product, proces, persoon, dienst of systeem dient te voldoen. Bij toepassing van deze normen, ontstaat vaak behoefte om door middel van een onafhankelijke beoordeling aan te tonen dat aan deze eisen wordt voldaan. Die beoordeling heet de certificatieaudit. Indien een product, dienst of proces in orde is bevonden, dan kan het product, de persoon of de organisatie een keurmerk of certificaat krijgen.

Is certificatie verplicht?

Certificatie is niet verplicht om aan de buitenwereld te kunnen aantonen dat een organisatie voldoet aan NEN 7510.

Moet je de organisatie laten certificeren om te voldoen aan NEN 7510?

Nee, certificatie is niet verplicht. Maar een zorginstelling moet wel kunnen aantonen dat zij voldoet aan NEN 7510. Certificatie is dé manier om dat te doen. NEN certificeert zelf niet. Dat gebeurt door certificerende instellingen, die op hun beurt weer onder toezicht staan van de Raad voor Accreditatie. Voor het certificeren tegen NEN 7510 is met een groot aantal certificerende instellingen (hierna CI) uniforme regels afgesproken. De certificatie tegen NEN 7510 wordt beoogd om onder accreditatie te laten plaatsvinden. Dat betekent dat de aangesloten CI's gebonden zijn aan een aantal strikte regels. Alleen een onafhankelijke CI mag de certificering uitvoeren. Daarnaast mag deze CI geen adviserende rol hebben in de te toetsen organisatie. En de CI staat onder toezicht van de Raad voor Accreditatie. Deze controleert of de CI handelt conform deze regels. De Raad voor Accreditatie baseert zich daarbij ook op internationale regelgeving. Meer over certificatie en accreditatie en de rol van NEN vindt u op de site van NEN.

Kunnen niet zorginstellingen zich laten certificeren tegen NEN 7510?

De primaire doelgroep van NEN 7510 zijn zorginstellingen. Zij kunnen zich laten certificeren tegen NEN 7510. Maar toeleveranciers, die met patiëntinformatie te maken hebben, kunnen zich ook laten certificeren tegen NEN 7510. Als deze toeleveranciers eveneens te maken hebben met andersoortige informatie, zoals financiële gegevens, dan kunnen zij zich ook nog laten certificeren tegen ISO 27001 'Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen'.

NEN 7510 en ISO 27001 gaan dus beide over informatiebeveiliging. De reikwijdte van certificatie wordt bepaald door het type informatie: wel of niet zorggerelateerd. Afhankelijk van het type informatie waar toeleveranciers mee te maken hebben, kunnen zij zich dus tegen NEN 7510 en/of ISO 27001 laten certificeren.

Moet in gebruik genomen software gecertificeerd zijn tegen NEN 7510?
Nee, het is de zorginstelling die aan NEN 7510 moet voldoen. Zij stelt een pakket van eisen samen en legt dit voor aan de softwareleverancier. De leverancier moet via specificaties kunnen aantonen dat hij voldoet aan de gestelde eisen.
Software die is geïntegreerd in een medisch hulpmiddel, moet voldoen aan de eisen van de Verordening medische hulpmiddelen (EU/2017/745). De fabrikant van een medisch hulpmiddel bepaalt door de 'intended use' van het medisch hulpmiddel te benoemen, in welke risicoklasse zijn product valt. Indien de software is geïntegreerd in het medisch hulpmiddel, dan valt deze software onder dezelfde risicoklasse als het medisch hulpmiddel. Stand-alone software wordt beschouwd als een actief medisch hulpmiddel, dat onder bepaalde voorwaarden tot risicoklasse IIa of IIb product wordt geclassificeerd .

Tegen welke norm kan ik me laten certificeren?

Zorginstellingen kunnen zich tegen NEN 7510 laten certificeren. De zorginstelling bepaalt zelf de reikwijdte van het te behalen certificaat. Dit kan bijvoorbeeld worden beperkt tot een specifieke afdeling en/of proces. Het is niet mogelijk om tegen NEN 7512 en NEN 7513 te certificeren. Deze normen zijn uitwerkingen van en toevoegingen op NEN 7510.

Wat betekent dat de norm NEN 7510 onder accreditatie staat?

Bij certificatie toetst een onafhankelijke certificerende instelling of het kwaliteitssysteem van een organisatie voldoet aan vooraf vastgestelde eisen. Hiermee wordt een strikte scheiding gerealiseerd tussen de partij de normen vastlegt (HKZ) en de toetsende instantie (de certificerende instelling). Deze scheiding is de basis voor een onafhankelijke en betrouwbare toetsing.

De Raad voor Accreditatie (RvA) is de gezaghebbende organisatie in Nederland die accreditaties verleent aan certificerende Instellingen. Voor certificatie onder accreditatie geldt een aantal strikte regels. Deze regels zijn opgenomen in NCS 7510. Certificerende instellingen die een contract afsluiten met NEN toetsen in overeenstemming met deze afspraken. De Raad voor Accreditatie controleert of deze afspraken worden nageleefd. Dat betekent dat de toetsing tegen deze norm onder accreditatie plaatsvindt. Toetsing onder accreditatie is gebonden aan een aantal strikte regels. Alleen een onafhankelijke certificerende instelling mag de certificering uitvoeren. Daarnaast mag deze certificerende instelling geen adviserende rol hebben in de te toetsen organisatie. De certificerende instelling staat onder toezicht van de Raad voor Accreditatie. Deze controleert of de certificerende instelling certificeringen volgens de regels uitvoert. De Raad voor Accreditatie baseert zich daarbij ook op internationale regelgeving.

Wat zijn de kosten van het certificatietraject?

In NCS 7510 ‘Conformiteitsbeoordeling - Eisen voor instellingen die audits ten behoeve van certificatie van informatiebeveiligingsmanagementsystemen in de zorg uitvoeren’ staan richtlijnen voor de wijze van toetsing en de auditordagen. Prijsopgaven van certificatietrajecten kunnen worden opgevraagd bij de aangesloten certificerende instellingen.

Checklist voor interne audit?

Een checklist voor interne audits kan een goed hulpmiddel zijn voor het stellen van de juiste vragen tijdens een audit als het niet teveel als een vaststaand keurslijf wordt gebruikt. Bijlage C van NEN 7510-2 geeft een goed handvat voor het soort van te stellen vragen.

Kan een organisatie ook worden gecertificeerd tegen NEN 7512 en NEN 7513?

Nee, een organisatie kan niet worden gecertificeerd tegen deze normen. En het ligt op dit moment niet voor de hand dat het voldoen aan NEN 7512-7513 kan worden ‘bewezen’ via een NEN 7510 audit. Mogelijk kan dit expliciet worden opgenomen in bijvoorbeeld de leveranciersovereenkomst en dat het in de periodieke overleg tussen de partijen wordt meegenomen.