Leidraad bij criterium 8b; Informatie voor klinieken en auditor

De kliniek moet compliant zijn met wet- en regelgeving betreffende privacy en informatieveiligheid (zoals NEN 7510)

2025
Juli 2025 toegevoegd een uitvoeringsplan voor auditoren

Doel Leidraad:
Handvat voor auditoren die de normeisen van het ZKN-keurmerk toetsen.
Deze leidraad is *niet bedoeld* als implementatiechecklist voor klinieken.

Elke kliniek is wettelijk verplicht om te voldoen aan de eisen uit de AVG[1] en NEN 7510[2]. Ook als de kliniek alle digitale producten en diensten heeft uitbesteed aan externe partijen.
Tijdens de audit voor het ZKN-keurmerk wordt compliance met NEN 7510 en de AVG (informatiebeveiliging en privacywetgeving) niet op inhoud getoetst. Tijdens deze audit moet het voor de ZKN-auditor echter wel duidelijk te beoordelen zijn of de kliniek voldoet aan wet- en regelgeving op deze onderwerpen. Hiervoor dient de kliniek een rapport van een onafhankelijke audit of certificering te laten zien en dienen de verbetermaatregelen terug te vinden zijn in de PDCA-cyclus.
Onderstaande informatie biedt auditoren van het ZKN-keurmerk houvast in de beoordeling van deze specifieke normeis 8b.

Waarom moet elke zorgaanbieder compliant zijn met de AVG en NEN 7510?
De gezondheidszorg is sterk afhankelijk van ICT, digitale producten, diensten en informatie. Tegelijk nemen de bedreigingen, zoals ransomware, toe. Informatiebeveiliging moet daarom op orde zijn. Verstoringen door problemen in de informatiebeveiliging of onverwachte gebeurtenissen, zoals stroomuitval, kunnen de continuïteit van zorg direct beïnvloeden. Ook kunnen gezondheidsgegevens lekken op het internet. Informatiebeveiliging is daarom een must. Vanuit wet- en regelgeving rondom informatiebeveiliging (die o.a. compliance met NEN 7510 verplicht) wordt dan ook verwacht dat zorgaanbieders *aantoonbaar* beschikken over een managementsysteem voor informatiebeveiliging dat voldoet aan de wettelijke norm. En ook dat er een continuïteitsplan is en dat dit regelmatig getest wordt.

Wat is NEN 7510?
NEN 7510 is de norm voor informatiebeveiliging in de zorg. Er staat in hoe organisaties in de zorg hun informatiebeveiliging moeten inrichten. De kern van NEN 7510 gaat over het managementsysteem voor informatiebeveiliging. Dit heet ook wel een ‘information securitymanagement system’ of ISMS. Verder beschrijft de norm een serie beheersmaatregelen. Hiermee kunnen organisaties hun risico’s wegnemen of kleiner maken.

Moet elke kliniek werken volgens NEN 7510?
NEN 7510 geldt sinds 2008 voor elke zorgaanbieder die gegevens van personen verwerkt in een zorginformatiesysteem, van universitair ziekenhuis tot huisarts of solistisch handelende tandarts. De kliniek moet kunnen laten zien dat er gewerkt wordt volgens NEN 7510. Dit volgt uit de Wet

[1] AVG = Algemene verordening gegevensbescherming
[2] NEN7510 = een Nederlandse norm die betrekking heeft op informatiebeveiliging in de gezondheidszorg. De normeisen en webtool zijn gratis te downloaden.

aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). De Regeling Gebruik Burgerservicenummer in de zorg verwijst eveneens expliciet naar NEN 7510. Dat geldt ook voor het Besluit elektronische gegevensverwerking door zorgaanbieders. Daarom moeten organisaties zich aan NEN 7510 houden bij het beheer, de beveiliging en het gebruik van een zorginformatiesysteem. Daarnaast is er de Algemene Verordening Gegevensbescherming (AVG). De AVG eist 'passende technische of organisatorische maatregelen' om persoonsgegevens te beschermen.

Wat betekent 'werken volgens NEN 7510'?
Werken volgens NEN 7510 betekent dat het information securitymanagement system (ISMS) goed werkt. De organisatie kan dan laten zien dat de PDCA-cyclus voor informatiebeveiliging werkt. Daarvoor is het niet genoeg dat er een beleid en beheersmaatregelen zijn. De organisatie moet ook controleren of ze werken zoals bedoeld. Als het nodig is moet de organisatie verbeteringen uitvoeren. NEN 7510 zegt dat de organisatie de informatiebeveiliging regelmatig onafhankelijk moet laten beoordelen.
In de AVG staat hoe organisaties moeten omgaan met persoonsgegevens. De AVG eist 'passende technische of organisatorische maatregelen' om persoonsgegevens te beschermen. NEN 7510 beschrijft zulke maatregelen. Maar u werkt alleen zoals bedoeld in NEN 7510 als u de informatiebeveiliging steeds controleert en verbetert. Daarvoor moeten er ook onafhankelijke beoordelingen zijn.

Wat zijn de voordelen van NEN 7510?
Het laat zien hoe de medewerkers van de kliniek omgaan met privacygevoelige informatie, het borgt de ontwikkeling en continuïteit van de organisatie van gegevensverwerking en het toont aan dat de kliniek vertrouwelijk en integer omgaat met patiëntengegevens.

Moet een kliniek een NEN 7510-certificaat hebben?
Nee. De wet stelt dit niet verplicht. NEN 7510 eist dit óók niet. Een NEN 7510-certificaat is één manier om te laten zien dat de kliniek werkt volgens de norm. Maar het is niet de enige manier. De kliniek dient tenminste information securitymanagement system (ISMS) en de beheersmaatregelen onafhankelijk te laten beoordelen (dit is niet hetzelfde als een certificering). Wél is het zo dat steeds meer gezamenlijke diensten rondom gegevensuitwisseling als eis stellen dat een zorginstelling NEN7510-gecertificeerd is of wordt.
Op deze pagina van NEN is te lezen welke instellingen NEN 7510 gecertificeerd zijn (inmiddels meer dan 4000) en welke instellingen NEN 7510 mogen certificeren.

Wanneer is de beoordeling onafhankelijk?
Bij een onafhankelijke beoordeling kijkt een expert naar het information securitymanagement system (ISMS) en de beheersmaatregelen. De expert moet iemand zijn met genoeg kennis van informatiebeveiliging en NEN 7510. De expert was/is niet zelf betrokken bij het opstellen van het informatiebeveiligingsbeleid van de kliniek en de uitvoering ervan. De expert kan een externe deskundige of een in audits gespecialiseerde organisatie zijn. Het kan ook een deskundig medewerker van een andere zorgorganisatie zijn.

Welke onderdelen moeten aan bod komen bij een onafhankelijke beoordeling?
- Het is duidelijk dat de beoordelaar deskundig en onafhankelijk is.
- In het rapport van de deskundige is de indeling van NEN 7510 duidelijk te herkennen. Dat betekent dat duidelijk is hoe het staat met:

    - Elk onderdeel van het information securitymanagement system (ISMS) (hoofdstukken 4 en verder van NEN 7510-1) en
    - De van toepassing zijnde beheersmaatregelen (bijlage A van NEN 7510-1).
- De auditor kijkt niet alleen naar de plannen op papier. De auditor kijkt ook naar (bewijs voor) hoe de informatiebeveiliging werkt in de praktijk.
- In het rapport van de deskundige NEN7510 staat:
    - Hoe de controle is uitgevoerd;
    - Met wie is gesproken (en in welke rol);
    - Welk bewijs is gebruikt;
    - Hoe het bewijs is verzameld.
    - Hoe de zorgaanbieder meet en bijstuurt, ook op de beheersmaatregelen uit bijlage A van NEN 7510.
- Het is duidelijk hoe de organisatie (ook in de toekomst) onafhankelijke beoordelingen regelt.

Is een éénmalige onafhankelijke beoordeling voldoende?
Nee. De norm gaat ervan uit dat een organisatie intern én extern de informatiebeveiliging laat beoordelen (zie o.a. onderdeel 18.1.1 in NEN 7510-2, resp. 5.31 in de komende versie van NEN 7510-2). Dit hoort bij een proces van steeds opnieuw verbeteren (de PDCA-cyclus). Omdat dit proces steeds doorgaat, zijn regelmatige interne en externe beoordelingen nodig. Hoe vaak is afhankelijk van de snelheid van wijzigingen in een organisatie.

Is het voldoende als de ICT-leverancier(s) werkt/werken volgens NEN 7510?
Nee. De kliniek blijft zélf verantwoordelijk voor de informatiebeveiliging. Ook de eigen bedrijfsprocessen binnen de kliniek hebben invloed op de informatieveiligheid. Bijvoorbeeld welke controles de kliniek doet als personeel wordt aangenomen of met ontslag gaat. Of wie binnen de kliniek toegang hebben tot informatiesystemen. Ook moet de kliniek de eisen voor informatiebeveiliging opnemen in de contracten met de leveranciers. Verder moet de kliniek de dienstverlening van de leveranciers beoordelen. Het kan voorkomen dat sommige beheersmaatregelen uit NEN 7510 niet nodig zijn, bijvoorbeeld als de kliniek zelf geen software ontwikkelt.

Hoe beoordeelt de auditor wanneer er sprake is van een tekortkoming?
Het is aan de auditor die het ZKN-keurmerk toetst om, op basis van bovenstaande informatie, te beoordelen in welke mate de kliniek compliant is met NEN 7510.
Let op, een 0-meting staat niet gelijk aan een interne audit.
De auditor zal een tekortkoming geven als een van deze zaken niet op orde is:
- Externe audit is niet uitgevoerd, maar gepland binnen 12 maanden (toetsbaar tijdens volgende ZKN-audit).
- Rapportage over uitkomsten interne audits is niet aanwezig, of verbetermaatregelen n.a.v. interne audits niet aantoonbaar opgenomen in plannen.

De auditor zal een kritische tekortkoming geven als een van deze zaken ontbreekt:
- Interne auditplanning voor compliance NEN 7510.
- Externe audit over meer dan 12 maanden gepland staat of nog helemaal niet gepland staat.

Periodiek uitvoeringsplan

Juli 2025

Periodiek Uitvoeringsplan voor Zelfstandige klinieken om te voldoen aan de eisen en richtlijnen binnen de kaders van de NEN 7510 en de AVG. Hierbij spelen privacy-persoonsgegevensbeveiliging en informatiebeveiliging een belangrijke rol. Alle hieronder vermelde acties voor auditoren houden direct verbinding met de wet- en regelgeving vanuit de NEN 7510 en AVG.

Bij onderstaand controleschema kan de auditor steeds de 3 kernvragen ter ondersteuning van de audit hanteren:

1. Gebruikt de organisatie haar geïmplementeerde ISMS-Tool afdoende om de risico's, de acties en beheersmaatregelen, alsmede de in-en externe audits op te volgen en na te leven?
2. Heeft de organisatie aantoonbaar de te nemen acties en/of beheersmaatregelen gekoppeld aan (eind)verantwoordelijken en zijn daar deadlines voor opgesteld. Met andere woorden zijn deze afdoende SMART geformuleerd?
3. Hoe en met welke frequentie en snelheid is de rapportage van de genomen acties en/of beheersmaatregelen gerapporteerd aan de Directie/Bestuur en verantwoordelijk management binnen de organisatie?

Onder het thema "leiderschap en verantwoordelijkheid" moet voor de auditor zichtbaar worden dat de directie/bestuurder van de kliniek zich eindverantwoordelijk voelt voor informatiebeveiliging zonder deze verantwoordelijkheid te delegeren.

Activiteit/Actielijst Uitvoeringskader NEN 7510	Wie verantwoordelijk	Aanpak	Borging	Frequentie controle
1. Risicoanalyse Toetsing op de beveiligingsrisico's met betrekking tot informatie-en persoonsgegevens binnen de organisatie.	Directie en Management	- Identificeren van de risico's op grond van bedreigingen en interne kwetsbaarheiden. - Beoordeling en documenteren van de impact en	- Implementeren van een Risicoregister voor vastlegging van de risico's. - Effectieve beheersmaatregelen koppel aan de geregistreerde risico's.	Periodiek en minimaal eens per jaar. Vaker indien nodig bijvoorbeeld bij: - introductie van nieuwe behandelingen of technologieën,

Activiteit/Actielijst Uitvoeringskader NEN 7510	Wie verantwoordelijk	Aanpak	Borging	Frequentie controle
		waarschijnlijkheid (realistisch). - Vaststellen en documenteren van mitigerende maatregelen in DPIA.	- Periodieke controle op de naleving van de genomen beheersmaatregelen	- wijzigingen in personeel of processen, - introductie van nieuwe behandelingen of technologieën, - wijzigingen in personeel of processen.
2. Data Protection Impact Assessment Houden van een DPIA om de risico's en de zwaarte en beheersing van de risico's daarvan goed in kaart te brengen. Essentieel bij verwerking van nieuwe persoonsgegevens met een hoog (privacy) risico (nieuw EPD-systeem, omzetten fysieke personeelsdossiers naar digitaal).	Directie en Management ICT Mogelijk Projectteam	- In kaart brengen van de gegevensstromen binnen de organisatie. - Beoordeling van de noodzaak en proportionaliteit. - Beschrijving en vastleggen van de risico's en genomen (beheers)maatregelen	- Gebruik van een zelfgekozen DPIA-template. - - Toetsing van de ingevulde DPIA door de (externe) Functionaris Gegevensbescherming en op de controle daarvan.	Eénmalig in de opstartfase en jaarlijks beoordelen en indien er wijzigingen plaatsvinden o.b.v. een hoog privacy risico
3. Interne Audit(s) of overige monitoring van processen Monitoring van processen is essentieel en moet continu plaatsvinden, ook in kleine organisaties. Moment van zelf-evaluatie. Houden van een onderlinge (interne) toetsing op alle processen binnen de organisatie m.b.t. informatie-en persoonsbeveiliging.	Directie en kwaliteitsfunctio-naris en/of SO/privacy officer	- Gebruik bijv. een format tijdens een interne audit. - Uitvoeren van onderlinge toetsing met andere vergelijkbare klinieken.	Opstellen van het interne auditrapport met daarin de bevindingen en verbeterpunten. - Registratie van de verbeterpunten, de genomen maatregelen en de monitoring van de opvolging daarop.	Jaarlijks beoordelen

Activiteit/Actielijst Uitvoeringskader NEN 7510	Wie verantwoordelijk	Aanpak	Borging	Frequentie controle
4. Awareness en Training Toetsing van de (aanwezige) bewustwording van alle medewerkers m.b.t. gebruik en beheersen van informatiebeveiliging. Trainen en educatie m.b.t. relevante richtlijnen binnen AVG. Ook de raad van bestuur/ bestuurder moet onderdeel uitmaken van het opleidingsplan	Directie en Management (interne opleidingen)	- Faciliteren en vaststellen opleidingsplan e-learning/workshops m.b.t. richtlijnen AVG Informatiebeveiliging en privacybeveiliging. - - Educatie/training m.b.t. praktijkvoorbeelden en incidenten omtrent informatiebeveiliging.	- Registratie deelname cursussen en trainingen in personeelsdossiers. - - Awareness onderdeel van de intake- en inwerkprocessen van nieuwe medewerkers.	Bij voorkeur half jaarlijks beoordelen
5. Beleid en procedures Actualisering van het interne beleid en hoe zijn de procedures gedocumenteerd binnen de organisatie m.b.t. informatiebeveiliging en privacy.	Directie en Management Kwaliteitsfunctionaris en/of SO /privacy officer	- Herzien en opnieuw toetsen van het geïmplementeerde Informatiebeveiligings beleid, de interne incidentenprocedure en het toegangsbeheer (borging autorisatie). - Het werken met een met een IT-leverancier die updates automatisch beheert en documenteert.	- Controle op de versiebeheer en het interne goedkeuringsproces van de relevante documenten. - Aantoonbaar actief communicatie en bewustwording van wijzingen naar de medewerkers (notulen werkoverleggen). - Het vastleggen in een procedure hoe updates worden beoordeeld en geïmplementeerd. - Het aantonen bij bijvoorbeeld audits dat de kliniek:	Jaarlijks beoordelen of bij wijziging van relevante wet- en regelgeving

Activiteit/Actielijst Uitvoeringskader NEN 7510	Wie verantwoordelijk	Aanpak	Borging	Frequentie controle
			- een actueel software-inventaris hebben - updates binnen redelijke termijn uitvoeren - Het vastleggen in een procedure hoe updates worden beoordeeld en geïmplementeerd. - Het aantonen bij bijvoorbeeld audits dat de kliniek: - een actueel software-inventaris hebben - updates binnen redelijke termijn uitvoeren	
6. Incidentmanagement Toetsing van registratie en opvolging van meldingen incidenten en/of calamiteiten m.b.t. de geïmplementeerde informatiebeveiliging. Incidentmanagement binnen een kliniek omvat álle soorten incidenten die impact kunnen hebben op de zorgkwaliteit, veiligheid, continuïteit of compliance, zoals: - Medische incidenten of bijna-incidenten - Klachten van patiënten - Technische storingen - Informatiebeveiligingsincidenten (zoals datalekken)	Directie en Management Kwaliteitsfunctionaris en/of SO/privacy-officer	- Stringente registratie van informatiebeveiligings-incidenten en de beschreven analyse/maatregelen daarop. - Uitvoeren van een “root cause analyses”	- Initiëren en gebruiken van een registratie-logboek meldingen incidenten/ - calamiteiten specifiek m.b.t. informatiebeveiliging (denk hierbij aan datalekken en meldingen aan de AP) - Periodiek evalueren en documenteren van zichtbare trends en verbeterpunten.	Per kwartaal beoordelen

Activiteit/Actielijst Uitvoeringskader NEN 7510	Wie verantwoordelijk	Aanpak	Borging	Frequentie controle
- Personele of organisatorische verstoringen				