DUIJNBORGH
CERTIFICATION

Certificering NEN 7510

NEN 7510 - 'Medische informatica - Informatiebeveiliging in de zorg'

is De Nederlandse norm die maatregelen beschrijft die zorginstellingen moeten nemen om op adequate wijze met persoonlijke gezondheidsinformatie om te gaan. Aan organisaties die indirect persoonlijke gezondheidsinformatie verwerken, zoals softwareleveranciers en hostingpartijen, wordt ook vaak gevraagd door middel van een NEN 7510 certificaat aan te tonen dat de noodzakelijke beveiligingsmaatregelen zijn getroffen.

Zekerheid op het gebied van de verwerking van persoonlijke gezondheidinformatie

Een goede beveiliging bij de verwerking van persoonlijke gezondheidsinformatie is niet allen van cruciaal belang, maar daarnaast ook nog eens wettelijk verplicht. Naast een goede beveiliging om te voorkomen dat onbevoegden kennis kunnen nemen van persoonlijke gezondheidsinformatie, zijn ook de integriteit (juistheid en volledigheid) en beschikbaarheid van persoonlijke gezondheidsinformatie erg belangrijk.

De Autoriteit Persoonsgegevens schroomt niet hoge boetes op te leggen aan (zorg) instellingen die hun zaakjes niet goed op orde hebben. Naast de imagoschade wilt u er natuurlijk niet aan denken dat persoonlijke gezondheidsinformatie, bewust of onbewust, door uw toedoen bij onbevoegden terecht komt met alle gevolgen van dien.

De breed geaccepteerde norm NEN 7510 biedt verwerkers van persoonlijke gezondheidsinformatie een procesgerichte aanpak voor het opzetten, implementeren, beheren, monitoren, evalueren, onderhouden en verbeteren van processen binnen een specifiek gebied.

De norm NEN 7510 is gebaseerd op de ISO 27001, aangevuld met een aantal *zorgspecifieke beheersmaatregelen*. Deze zorgspecifieke aanscherpingen zijn van het dwingende 'moeten' ('shall') voorzien op basis van een universele risicobeoordeling voor de zorg.

Door de invoering van NEN 7510 laat u betrokken partijen, zoals patiënten, toezichthouders en medewerkers, zien dat u aandacht heeft voor het belang van:
- het vertrouwelijk omgaan met persoonlijke gezondheidsinformatie,
- het beschikbaar hebben van persoonlijke gezondheidsinformatie wanneer dat gewenst is en,
- persoonlijke gezondheidsinformatie die accuraat en volledig is.

Waarom Duijnborgh Certification?

Wij zijn een certificerende instantie, gespecialiseerd in certificeringen op het gebied van ICT. Wij zijn op grond van de Wet aanwijzing nationale accreditatie-instanties door de Raad voor Accreditatie (RvA) geaccrediteerd voor certificering tegen de ISO-IEC 27001 norm (ook bekend onder de naam Code voor informatiebeveiliging). Ook voor andere ICT gerelateerde normen zoals de NEN 7510, de ISO 27017, ISO 27018, ISO 27701, ISO 20000, ISO 22399 en de ISO 25010 kunt u bij ons terecht. Wij zijn geen 'certificeringsfabriek', noch krijgt u bij ons het certificaat 'kado'. Als u -samen met ons- de overtuiging heeft dat certificatie geen doel op zichzelf is, maar een middel om te komen tot betere bedrijfsprestaties, dan bent u bij ons aan het goede adres.

De norm NEN 7510 (‘Medische informatica - Informatiebeveiliging in de zorg’)

Het invoeren van een informatiebeveiligingsbeheerssysteem is geen doel op zichzelf. Redenen kunnen extern gestuurd zijn zoals een eis van een toezichthouder of van een organisatie die diensten uitbesteedt, of intern gestuurd vanuit de wens om de vertrouwelijkheid en integriteit van gevoelige bedrijfsinformatie en de bedrijfscontinuïteit te borgen. Door de opzet van de NEN 7510 norm is deze geschikt voor elke organisatie, groot of klein, in welke sector of welk deel van de wereld dan ook. De norm is primair van belang voor sectoren waar de beveiliging van persoonlijke gezondheidsinformatie cruciaal is, zoals in de eerste en tweedelijns gezondheidszorg, maar ook voor andere organisaties die - direct of indirect - persoonlijke gezondheidsinformatie verwerken.

De aanpak van Duijnborgh Certification

Als geen ander weet Duijnborgh Certification dat het opzetten van een systeem volgens generieke eisen niet zomaar past bij uw unieke organisatie. Samen met u zoeken wij naar de meerwaarde van het beheerssysteem om relevante activiteiten te beheersen en te verbeteren. Eerst worden de wensen van uw organisatie en eventuele stakeholders in kaart gebracht. Op basis van het resultaat zal een offerte worden uitgebracht.

Vanuit een (facultatieve) proefbeoordeling kan de organisatie een indruk krijgen over de status van haar informatiebeveiliging en beslissen om wel of niet een certificatietraject in te gaan of een geschikt tijdspad te bepalen voor certificering.

Gefaseerde aanpak

Het certificeringtraject zelf wordt uitgevoerd in 2 fasen waarbij per fase een rapportage wordt opgeleverd met daarin de conclusie, tekortkomingen, verbetersuggesties en aandachtpunten voor het management.

Fase 1 - Tijdens fase 1 van het certificeringtraject wordt het gedocumenteerde beheerssysteem van de organisatie beoordeeld. Het gaat hierbij om de methode van risicoanalyse, de Verklaring van Toepasselijkheid en de aanwezigheid en werking van de kernelementen van het beheerssysteem. Eventuele tekortkomingen dienen voor fase 2 te zijn opgepakt.

Fase 2 - Tijdens fase 2 van het certificeringtraject wordt beoordeeld of het gedocumenteerde systeem van de organisatie in voldoende mate is ingevoerd en het beheerssysteem ondersteunt. Het beheerssysteem dient in overeenstemming met de eisen uit de NEN 7510, zoals eigen beleid, vigerende wet- en regelgeving en eisen van belanghebbenden te functioneren en in staat te zijn om continue te verbeteren en onderkende risico’s te minimaliseren.

Op basis van de resultaten uit fasen 1 en 2 zal worden besloten of er overgegaan wordt tot certificering en het verstrekken van het certificaat. Indien er (nog) onvoldoende aan de eisen vanuit de norm wordt voldaan dient de organisatie maatregelen te treffen. Na het corrigeren van de tekortkomingen, kan het resultaat worden geëvalueerd en alsnog worden overgegaan tot certificering.

Een certificaat is drie jaar geldig, waarbij het beheerssysteem minimaal jaarlijks wordt geëvalueerd.

Duijnborgh Certification BV
WTC Papendorp
Papendorpseweg 100
3528 BJ Utrecht
T 31(0)88 160 1750
F 31(0)88 160 1799
E info@dbcert.nl

DUIJNBORGH CERTIFICATION®