Waarom NEN 7510 certificeren?

Wat is een NEN 7510 audit en waarom is deze belangrijk voor uw organisatie?

Alle zorgaanbieders in Nederland moeten sinds januari 2018 aan de NEN 7510 voldoen, conform het besluit Elektronische gegevensverwerking Zorgaanbieders.

In deze wet staat ook dat organisatie moeten voldoen aan de NEN 7512 en NEN 7513. Immers, de elektronische gegevensverwerking moet veilig plaatsvinden (NEN 7512), maar activiteiten moeten ook zorgvuldig worden gelogd (NEN 7513).

In de wet staat dat zorgorganisaties aan deze normen moeten voldoen. Wat er niet staat is dat de organisaties gecertificeerd moeten zijn. Echter, gebaseerd op de inhoud van de meest recente brieven van het Ministerie van Volksgezondheid, Welzijn en Sport betreffende aanstaande e-Health regels, zal het een kwestie van tijd zijn voordat een NEN 7510 certificering verplicht wordt gesteld. Een certificering wordt dan ook sterk aanbevolen door de Nederlandse Vereniging van Ziekenhuizen (NVZ) waarmee wij samenwerken.

Nu al belangrijk voor IGJ en AP

Een NEN 7510 certificering is nu ook al belangrijk voor alle zorgaanbieders. De Inspectie Gezondheidszorg en Jeugd (IGJ) beoordeelt zorgaanbieders op vele punten, waaronder de NEN 7510. Indien blijkt dat hieraan niet wordt voldaan, dan geeft het IGJ direct een termijn voor correctie en onpartijdige aantoonbaarheid van het voldoen aan de NEN 7510. Verder werkt IGJ samen met de Autoriteit Persoonsgegevens (AP). Mocht er onverhoopt een datalek optreden, dan is het hebben van een NEN 7510 certificering belangrijk. Immers, als bestuur kunt u hiermee aantonen dat u er alles aan heeft gedaan om de informatiebeveiliging op orde te hebben en te houden.

Om dit paniekvoetbal te voorkomen, zien we dat het bestuur van steeds meer zorgaanbieders er zelf voor kiest om het NEN 7510 certificeringstraject te starten.

Audit

Zonder een onafhankelijke audit uitgevoerd door een certificerende instelling is het niet mogelijk om de certificering te verkrijgen. Het is dé manier om aan te tonen dat u een goed werkend managementsysteem voor informatiebeveiliging heeft.

De initiële audit bestaat uit een fase 1 en een fase 2 beoordeling. Tijdens fase 1 beoordeling kijken we al of het managementsysteem voor informatiebeveiliging goed functioneert. Werkt de PDCA? Bij een goed resultaat gaat u door naar de fase 2 beoordeling. In deze fase toetsen we het gehele managementsysteem en kijken we goed naar alle beheersmaatregelen. Zijn deze conform uw eigen risicoanalyse zorgvuldig ingericht? Zijn de uitgangspunten met betrekking tot Beschikbaarheid, Integriteit en Vertrouwelijkheid van de informatie zorgvuldig ingeregeld?

Als de audit positief wordt afgesloten dan wordt u ‘voorgedragen’ voor certificering. De certificatiemanager van onze organisatie beoordeelt normaals het dossier; een soort peer-review. Indien alles op orde is, wordt uw managementsysteem voor informatiebeveiliging gecertificeerd.

We komen dan graag langs om het certificaat uit te reiken.

NEN 7510 auditor

De NEN 7510 auditor beoordeelt het gehele managementsysteem voor informatiebeveiliging en alle genomen beheersmaatregelen. Daarmee toont u aan de buitenwereld aan dat uw organisatie voldoet aan de strenge richtlijnen en voorwaarden op het gebied van informatiebeveiliging.

Tijdens de audit is de context van de zorgorganisatie leidend. Immers, een GGD is bijvoorbeeld anders dan een ziekenhuis of een specialistische kliniek.

Onze NEN 7510 auditoren komen uit de zorg en voelen daarom uw organisatie goed aan. Wij auditen scherp, maar zadelen u niet op met zaken die niet relevant zijn binnen de context van uw organisatie.

NEN 7510 audit checklist

Wilt u weten of u al klaar bent voor certificeren of wilt u weten waar u staat met betrekking tot de NEN 7510 eisen? Vraag dan onze checklist aan.

Uiteraard kunnen we naast deze checklist ook een nul-meting of pre-audit uitvoeren. Tijdens deze audit kijken we goed naar uw managementsysteem voor informatiebeveiliging en naar de 114 beheersmaatregelen uit de NEN 7510-2.