ISO 27799

INFORMATIEBEVEILIGINGSBEHEER IN DE GEZONDHEIDSZORG

SGS.NL

SGS

ISO 27799
Het alternatief voor NEN 7510

Tegenwoordig is er steeds meer aandacht voor informatie-beveiliging. Dit komt omdat veel organisaties dagelijks te maken hebben met vertrouwelijke en/of privacygevoelige gegevens. Het is essentieel dat deze informatie niet op straat terecht komt.

Dit geldt zeker ook voor de zorgsector, waar steeds meer informatie bewaard en uitgewisseld wordt. Deze informatie is altijd vertrouwelijk van aard, denk daarbij aan patiëntgegevens en data over medische aandoeningen en behandelingen.

Elke zorgorganisatie dient daarom zeker te stellen dat er zorgvuldig en integer wordt omgegaan met vertrouwelijke en/of privacygevoelige gegevens.

INFORMATIEBEVEILIGINGSSYSTEEM

Elke organisatie moet voorkomen dat vertrouwelijke en/of privacygevoelige gegevens beschikbaar komen voor onbevoegde personen/partijen. Dit komt enerzijds door wet- en regelgeving waar zij aan moet voldoen op het gebied van privacy-bescherming, zoals de GDPR-wetgeving. Anderzijds vragen hun stakeholders steeds vaker naar aantoonbaar bewijs dat er vertrouwelijk en integer omgegaan wordt met vertrouwelijke en/of privacygevoelige gegevens.
Er zijn systemen ontwikkeld om het vertrouwelijksheidvraagstuk adequaat te kunnen beantwoorden.

INFORMATIEBEVEILIGINGSNORMEN

Het toepassen van normen op het gebied van informatiebeveiliging ondersteunen organisaties:

- Doordat ze met hun raamwerk en eisen helpen bij het opzetten van een Informatiebeveiligings-systeem (ISMS).
- Ze vragen om beheers-maatregelen op basis van een risicoanalyse te implementeren.
- Ze leveren aantoonbaar bewijs dat een organisatie op een verantwoorde wijze omgaat met vertrouwelijke gegevens.

AANTOONBAARHEID

Managementsystemen kunnen getoetst worden door middel van een audit door een certificerende instelling (CI). Tijdens de certificatieaudit wordt getoetst of het informatiebeveiligingssysteem en de daarbij behorende processen goed functioneren en bveiligd zijn.

Als dat op orde is, ontvangt de organisatie aantoonbaar bewijs, in de vorm van een ISMS-certificaat, dat de informatiebeveiliging goed beheerst wordt.

Het ISMS-certificaat kan door organisaties gebruikt worden bij aanbestedingen. Of als erkenning naar klanten en stakeholders dat de organisatie goed omgaat met vertrouwelijke en/of privacygevoelige gegevens

GEZONDHEIDSZORG

Patiëntgegevens en data over medische aandoeningen zijn voor zorgverleners een belangrijk wapen tegen dubbele onderzoeken en medische fouten. Deze informatie is vrijwel altijd vertrouwelijk van aard.

Doordat in de zorgsector steeds meer vertrouwelijke informatie bewaard en uitgewisseld wordt, liggen deze organisaties onder een vergrootglas als het gaat om de manier hoe ze met data omgaan. Het is daarom niet vreemd dat zorgverleners steeds meer aandacht besteden aan informatieverwerking binnen en buiten hun organisatie.

Veel zorgverleners vragen daarom om aantoonbaar bewijs. Dit kan geleverd worden in de vorm van ISO 27799 certificering, in combinatie met ISO 27001.

ISO 27799 VOOR DE ICT-SECTOR

De NEN 7510-norm is niet alleen geschikt voor zorginstellingen. Zo komen ICT-leveranciers die actief zijn in de zorgsector ook in aanraking met patiëntgegevens. Daarom richt de NEN 7510 zich op de gehele zorgketen, van individuele zorgverleners tot grote zorginstellingen, software-ontwikkelaars, hostingbedrijven, toeleveranciers als netwerkorganisaties, cloud providers, aanbieders van SaaS IT-oplossingen en zorgverzekeraars.

NEN 7510

De combinatie van ISO 27799 en ISO 27001, is het internationale equivalent van de NEN 7510.

Deze combinatie oplossing beschrijft maatregelen die zorginstellingen en toeleveranciers moeten nemen om op adequate wijze met patiëntgegevens om te gaan.

Deze maatregelen zorgen ervoor dat informatiebeveiliging een gecontroleerd proces wordt en dat het proces betrekking heeft op alle verschijningsvormen waarin patiëntgegevens zijn vastgelegd.

De beveiligingseisen gelden voor de informatie binnen de zorginstelling, maar ook voor de informatie die organisaties onderling uitwisselen.

De combinatie ISO 27799 en ISO 27001 is in principe geschikt voor elke organisatie in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces. Denk daarbij aan zorginstellingen, maar ook aan alle organisaties die persoonlijke gezondheidsinformatie verwerken zoals ICT-dienstverleners en applicatieontwikkelaars.

ISO 27001 & ISO 27799

De ISO 27001-norm is dé wereldwijde standaard voor informatiebeveiliging.

Doormiddel van ISO 27001-certificering tonen organisaties aan dat zij de juiste beheersmaatregelen treffen om gegevens te beveiligingen. Onder andere door de beschikbaarheid, integriteit en vertrouwelijkheid van deze gegevens te waarborgen.

Daarnaast voldoet uw organisatie met de ISO 27799 aantoonbaar aan de IGZ-eisen.

PATIËNTGEGEVENS BEVEILIGEN

In Nederland is de NEN 7510 een bekende norm bij organisaties die betrokken zijn bij de leveringsketen in de zorg.
Een van de redenen hiervoor is dat de NEN 7510 in wet- en regelgeving wordt genoemd . Conform de 'Regeling gebruik Burgerservicenummer in de zorg' moeten zorgorganisaties voldoen aan de eisen zoals die in de NEN 7510 worden benoemd. Met de combinatie ISO 27001 en ISO 27799 voldoet u aan deze eisen.

Bescherm vertrouwelijke gegevens met ISO 27001 en ISO 27799

IS NEN 7510 VERPLICHT VOOR ZORGAANBIEDERS OF HUN LEVERANCIERS?

Veel zorgorganisaties stellen NEN 7510 als eis. Het is echter vanuit de ‘Regeling gebruik Burgerservicenummer in de zorg’ niet verplicht om te kiezen voor NEN 7510. Verwerkingsverantwoordelijken hebben een verantwoordingsplicht. Dat betekent dat een organisatie aan moeten kunnen tonen dat zij de juiste organisatorische en technische maatregelen heeft genomen om invulling te geven aan de NEN 7510.

De Inspectie voor de Gezondheidszorg (IGZ) gebruikt in Nederland de NEN 7510 als leidraad om te toetsen of zorginstellingen hun informatiebeveiliging goed hebben geregeld en geborgd.

Organisaties in de gezondheidszorg zijn dus niet verplicht om NEN 7510 gecertificeerd te zijn.

ISO 27799

ISO 27799 is een internationale norm die richtlijnen geeft voor een informatiebeveiligingsbeheersysteem. De norm is, net zoals de NEN 7510, geschikt voor elke organisatie in de gezondheidszorg, ongeacht de aard en de omvang van het bedrijfsproces. Zorginstellingen, maar ook alle organisaties zoals ICT-dienstverleners en applicatieontwikkelaars (PGO’s) die persoonlijke gezondheidsinformatie verwerken, kunnen gebruik maken van deze norm.

In Nederland heeft het Nederlands Normalisatie-instituut (NEN) de ISO 27799-norm als basis gebruikt voor de ontwikkeling van de NEN 7510.

SGS biedt de combinatie ISO 27001 en ISO 27799-certificering aan als volwaardig equivalent voor de NEN 7510.

In combinatie met ISO 27001 biedt ISO 27799-certificering aantoonbaar bewijs dat organisaties voldoen aan de ‘Regeling gebruik Burgerservicenummer in de zorg’.

Voldoe aan de 'Regeling gebruik burgerservicenummer in de zorg' met ISO 27799.

BELANGRIJK OM TE WETEN

Voldoen aan de eisen van NEN 7510 wordt in de wet genoemd, dit is echter geen verplichting voor een zorginstelling of hun leveranciers, daar waar patiëntgegevens worden verwerkt. Met de combinatie ISO 27001 en ISO 27799 voldoet u aan de eisen zoals in de wet genoemd.

Werken conform de combinatie ISO 27001 en ISO 27799 is een verplichting bij zorginstellingen of hun leveranciers zodra er patiëntgegevens worden verwerkt.

Vanuit wet- en regelgeving is er druk op de zorg-instellingen en hun leveranciers om te voldoen aan de normelementen uit de combinatie ISO 27001 en ISO 27799

Zorginstellingen of hun leveranciers voldoen aan de ‘Regeling gebruik Burgerservicenummer in de zorg’ zodra men de normen ISO 27001 en ISO 27799 naleeft.

WWW.SGS.COM

CONTACTINFORMATIE

be.ssc.sales@sgs.com
nl.certificatie@sgs.com

t +32 (0)3 545 48 48
t +31 (0)88 214 37 88

www.sgs.com/linkedin

WHEN YOU NEED TO BE SURE