Digital Security
Progress. Protected.

ESET FOR HEALTHCARE
Een digitale hartstilstand voorkomen

Digital Security voor de gezondheidszorg

DIT ZIJN DE BELANGRIJKSTE WETGEVINGEN VOOR DE ZORG:

Algemene Verordening Gegevensbescherming (AVG)

Dit gaat over het beschermen van de privacy en beveiliging van persoonsgegevens

Wet Geneeskundige Behandelovereenkomst (WGBO)

Dit gaat over het inzagerecht van patiënten in hun eigen medisch dossier en de verplichting om een medisch (digitaal) dossier bij te houden.

NIS2

Wetgeving waarbij de aanbieder van essentiële diensten moet kunnen aantonen dat zij voldoen aan de organisatorische en technische eisen van NIS2

DIT IS HET BELANGRIJKSTE NORMENKADER IN DE ZORG:

NEN7510 norm

Normenkader voor het informatiebeveiligingsbeleid

DIT ZIJN DE BELANGRIJKSTE ONDERWERPEN VOOR ZORGAANBIEDERS:

Elektronisch Patiëntendossier

Veilig uitwisselen van gezondheidsgegevens tussen zorgverleners en patiënten

Ransomware, Phishing, IoT/OT, BYOD, Cloud en Privacy

ESET for healthcare

Een speciale rol voor cybersecurity coördinatie in de zorg is weggelegd voor Z-Cert. Z-Cert is een onafhankelijke stichting die is opgericht om de digitale weerbaarheid van de zorgsector in Nederland te vergroten. Z-Cert biedt zorginstellingen verschillende diensten aan om hen te ondersteunen bij het verbeteren van hun digitale veiligheid en om te voldoen aan relevante wet- en regelgeving.

De belangrijkste rol van Z-Cert is het bevorderen van digitale weerbaarheid in de zorgsector.
Dit doet Z-Cert onder andere door:

- Het bieden van expertise op het gebied van informatiebeveiliging en privacy voor zorginstellingen.
- Het uitvoeren van audits en controles om de digitale veiligheid van zorginstellingen te verbeteren en te waarborgen.
- Het ontwikkelen van richtlijnen, normen en standaarden op het gebied van informatiebeveiliging in de zorg.
- Het bieden van trainingen en workshops aan zorginstellingen om hun medewerkers bewust te maken van de risico's van cyberdreigingen en hoe ze zich daartegen kunnen beschermen.
- Het fungeren als een centraal meldpunt voor beveiligingsincidenten en datalekken in de zorgsector.

Zorginstellingen kunnen bij Z-Cert terecht voor ondersteuning bij het verbeteren van hun digitale veiligheid en het voldoen aan wet- en regelgeving, waaronder de NEN 7510 en de AVG. Z-Cert is een belangrijke partner voor de zorgsector in Nederland en helpt bij het verbeteren van de digitale weerbaarheid van deze sector.

AVG

Om de Algemene Verordening Gegevensbescherming (AVG) na te leven, moet een zorginstelling aan een aantal eisen voldoen. Hieronder geef ik een overzicht van de belangrijkste eisen.

1. **Transparantie en informatieverstrekking:** Zorginstellingen moeten transparant zijn over hoe zij persoonsgegevens verwerken en moeten betrokkenen hierover informeren.
2. **Rechtmatigheid en doelbinding:** Zorginstellingen mogen persoonsgegevens alleen verwerken als dit rechtmatig is en als zij dit doen voor een welbepaald doel. Zij moeten de gegevens ook alleen verwerken voor dit specifieke doel.
3. **Dataminimalisatie:** Zorginstellingen mogen alleen die persoonsgegevens verwerken die noodzakelijk zijn voor het doel waarvoor ze verwerkt worden.
4. **Beveiliging van persoonsgegevens:** Zorginstellingen moeten technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen tegen ongeautoriseerde toegang, verlies of diefstal.
5. **Meldplicht datalekken:** Als er sprake is van een datalek, dan moet een zorginstelling dit melden aan de Autoriteit Persoonsgegevens en, in sommige gevallen, ook aan betrokkenen.
6. **Rechten van betrokkenen:** Betrokkenen hebben een aantal rechten, waaronder het recht op inzage, rectificatie, verwijdering en dataportabiliteit. Zorginstellingen moeten ervoor zorgen dat betrokkenen deze rechten kunnen uitoefenen.
7. **Functionaris voor gegevensbescherming:** Als een zorginstelling op grote schaal persoonsgegevens verwerkt, dan moeten zij een functionaris voor gegevensbescherming (FG) aanstellen. De FG houdt toezicht op de naleving van de AVG.

Het is belangrijk om op te merken dat de AVG ook van toepassing is op de verwerking van gezondheidsgegevens, omdat dit als bijzondere categorie persoonsgegevens wordt beschouwd. Zorginstellingen moeten daarom extra voorzichtig zijn bij het verwerken van gezondheidsgegevens en ervoor zorgen dat zij aan alle eisen van de AVG voldoen.

WGBO

De Wet Geneeskundige Behandelovereenkomst (WGBO) regelt de relatie tussen zorgverlener en patiënt en heeft onder meer betrekking op de verwerking van persoonsgegevens in de gezondheidszorg. Het gaat dan om gevoelige informatie over de gezondheid van een patiënt, die zorginstellingen zorgvuldig moeten verwerken en beschermen. Technische maatregelen die een zorginstelling kan nemen om te voldoen aan de WGBO zijn:

1. **Beveiliging van persoonsgegevens:** Zorginstellingen moeten technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen ongeautoriseerde toegang, verlies of diefstal. Denk bijvoorbeeld aan het versleutelen van gegevens, het implementeren van toegangscontrole en het beveiligen van de netwerken en systemen.
2. **Gebruik van veilige communicatiemiddelen:** Zorginstellingen moeten veilige communicatiemiddelen gebruiken om persoonsgegevens te verzenden, bijvoorbeeld bij het delen van medische gegevens tussen verschillende zorgverleners. Dit kan bijvoorbeeld door het gebruik van versleutelde e-mails of secure messaging.
3. **Bewaartermijnen:** Zorginstellingen moeten persoonsgegevens niet langer bewaren dan nodig is voor het doel waarvoor zij zijn verzameld. Het is belangrijk om deze bewaartermijnen goed te documenteren en de gegevens op een veilige manier te bewaren, bijvoorbeeld door middel van back-ups en archiveringssystemen.
4. **Inzet van veilige software en systemen:** Zorginstellingen moeten zorgvuldig kiezen welke software en systemen zij gebruiken voor de verwerking van persoonsgegevens. Het is belangrijk om te zorgen dat deze software en systemen voldoen aan de AVG en andere relevante wet- en regelgeving op het gebied van gegevensbescherming.
5. **Monitoren van beveiligingsincidenten:** Zorginstellingen moeten beveiligingsincidenten monitoren en snel reageren als er iets misgaat. Het is daarom belangrijk om een adequaat beveiligingsincidenten- en responsplan te hebben en deze regelmatig te testen.

Het is belangrijk om op te merken dat technische maatregelen alleen niet voldoende zijn om te voldoen aan de WGBO. Zorginstellingen moeten ook organisatorische maatregelen nemen, zoals het opstellen van heldere protocollen voor de verwerking van persoonsgegevens en het geven van trainingen aan medewerkers over gegevensbescherming en privacy.

NEN 7510

Om NEN 7510 gecertificeerd te worden moet een zorginstelling voldoen aan de normen die zijn vastgelegd in de NEN 7510. Deze norm is een Nederlandse norm voor informatiebeveiliging in de zorgsector en bevat specifieke eisen voor de bescherming van medische gegevens. De norm bestaat uit twee delen:

1. **Deel 1:** Algemene eisen voor informatiebeveiliging in de zorgsector.
   Dit omvat eisen voor beleid, organisatie, personeel, fysieke beveiliging, toegangsbeveiliging, continuïteitsplanning, risicomanagement en beveiligingsmaatregelen.
2. **Deel 2:** Aanvullende eisen voor elektronische gegevensuitwisseling tussen zorginstellingen.
   Dit deel omvat eisen voor authenticatie, autorisatie, encryptie, logging en controle van gegevensuitwisseling.

Enkele voorbeelden van eisen die gesteld worden in de NEN 7510 zijn:

- Een informatiebeveiligingsbeleid dient te worden opgesteld en regelmatig geëvalueerd.
- Personeel dient een geheimhoudingsverklaring te ondertekenen en regelmatig getraind te worden op informatiebeveiliging.
- Er moet een proces zijn voor het beoordelen van risico's en het nemen van beveiligingsmaatregelen.
- Er moeten procedures zijn voor de beveiliging van de fysieke omgeving en de toegang tot gegevens.
- Er moeten maatregelen worden genomen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen, bijvoorbeeld door middel van encryptie en backups.
- Er moet een logging- en controleproces zijn om te controleren wie toegang heeft tot welke informatie.

Als een zorginstelling voldoet aan de normen van de NEN 7510 en slaagt voor een audit door een certificerende instelling, kan zij een NEN 7510-certificaat ontvangen. Dit certificaat toont aan dat de zorginstelling voldoet aan de normen voor informatiebeveiliging in de zorgsector.

NIS2

De eisen voor zorginstellingen die aan de NIS2 willen voldoen, kunnen in grote lijnen worden onderverdeeld in twee categorieën: organisatorische eisen en technische eisen. Hieronder zie je een overzicht van de belangrijkste eisen.

Organisatorische eisen:

1. Risicoanalyse en beveiligingsbeleid: Zorginstellingen moeten een risicoanalyse uitvoeren en op basis hiervan een passend beveiligingsbeleid formuleren en implementeren.
2. Continuïteitsplanning: Zorginstellingen moeten een continuïteitsplan opstellen om de beschikbaarheid van hun diensten te waarborgen in geval van een incident.
3. Incidentbeheer: Zorginstellingen moeten een procedure hebben voor het detecteren, melden, analyseren en oplossen van incidenten op het gebied van informatiebeveiliging.
4. Training en bewustwording: Zorginstellingen moeten hun medewerkers regelmatig trainen en bewust maken van de risico's van cyberdreigingen en de maatregelen die zij moeten nemen om deze te voorkomen.

Technische eisen:

1. Netwerkbeveiliging: Zorginstellingen moeten zorgen voor een veilige configuratie en beheer van hun netwerkapparatuur, zoals routers, switches en firewalls.
2. Systeembeveiliging: Zorginstellingen moeten hun systemen, zoals servers en werkstations, beveiligen tegen ongeautoriseerde toegang en malware.
3. Toegangsbeheer: Zorginstellingen moeten een strikt toegangsbeleid voeren voor hun IT-systemen en -diensten, met als doel om ongeautoriseerde toegang te voorkomen.
4. Logging en monitoring: Zorginstellingen moeten logging- en monitoringtools implementeren om inzicht te krijgen in de activiteiten op hun IT-systemen en -diensten en verdachte activiteiten te detecteren.

Het is belangrijk om op te merken dat de eisen van de NIS-richtlijn 2 niet alleen betrekking hebben op technische maatregelen, maar ook op organisatorische en procedurele maatregelen. Zorginstellingen moeten daarom een alomvattende aanpak hanteren om aan de eisen van de NIS-richtlijn 2 te voldoen.