Informatieveiligheid in de zorg

INZICHT IN UW DIGITALE VEILIGHEID

Secura heeft meer dan twee decennia ervaring in informatiebeveiliging en privacy op het gebied van mensen, processen, techniek en organisatie. Wij identificeren IT-beveiligingsrisico's vanuit een onafhankelijk standpunt, waarbij het hoogste niveau van vertrouwelijkheid en integriteit behouden blijft. Dit stelt u in staat om proactief de controle te houden over de eigen digitale veiligheid.

Nulmeting NEN 7510 & Gedragslijn Audit 1.0

Ziekenhuizen hebben informatieveiligheid hoog op de agenda staan. Samenwerkingsorganen en toezichthouders spelen hierop in. **De Nederlandse Vereniging van Ziekenhuizen (NVZ) heeft een Routekaart opgesteld** en deze opgenomen in een beleidskader om als sector stappen te kunnen zetten. **Het einddoel is een sector brede kwaliteitsverbetering te realiseren naar minimaal het niveau van de NEN 7510 standaard**. Dit sluit aan op de eis te voldoen aan de NEN 7510 standaard (en aansluitende standaarden) die is vastgelegd in een wettelijk besluit en regeling.

De Routekaart vraagt om twee stappen waarmee Secura u graag helpt:

1. De NEN 7510 Nulmeting
2. De Gedragslijn Audit 1.0 ofwel 1-meting

Daarnaast kan Secura u in brede zin ondersteunen bij het zekerheid krijgen over de status en implementatie van de beheersingsmaatregelen gericht op het voldoen aan de NEN 7510 richtlijnen, waaronder awareness en veilig gedrag.

NEN 7510 Nulmeting

Met een nulmeting kan een organisatie aantonen dat zij 'in control' is op informatieveiligheid en/of inzichtelijk krijgen waar nog verbeteringen zijn te realiseren. De standaard hiervoor is de NEN 7510. Deze nulmeting beslaat 4 stappen:

1. **Start** - Kick-off & Scope
2. **Meten** - Inventarisatie
3. **Analyse** - Onderzoeken
4. **Rapporteren** - Rapportage & Evaluatie

In de rapportage vindt u de **belangrijkste bevindingen samengevat en de samenhangende risico's toegelicht met een heat map**. Deze heat map ondersteunt bij het prioriteren van verbetermaatregelen en het inzichtelijk maken van verbeteringen aan de hand van de deltametingen. Samen met de auditor stelt de organisatie een actiepunten lijst op. De integrale bevindingen en acties zijn opgenomen in een bijlage en worden verstrekt in een Excelbestand.

1. Start

Kick-off & Scope
- Scope bepaling
- Centrale afstemming proces en inhoud
- Overzicht documentatie
- Planning
- Opzet 'Secure exchange'

2. Meten

Inventarisatie
- Vragenlijsten
- Bewijsstukken
- Interviews
- Deelwaarnemingen
- Data verzamelen
- Scans

3. Analyse

Onderzoeken
- Analyse documenten
- Steekproeven
- Directe waarneming
- Data analyse

4. Rapporteren

Rapportage & Evaluatie
- Bevindingen
- Afstemming
- Risico's
- Aanbevelingen
- Volwassenheidsniveau
- Actielijst

Aanpak nulmeting

De Secura aanpak hebben wij hier kort geschetst.

- De betrokkenheid van medewerkers van de klantorganisatie in de audit is cruciaal. Daarom start de audit met een **kick-off**. Met inzet van meerdere controlemiddelen vindt de inventarisatie van maatregelen plaats.
- De auditor **analyseert de uitkomsten en verricht nog aanvullend controlewerk** waaronder het toetsen van het bestaan van maatregelen.
- Alvorens te rapporteren vindt **afstemming plaats over de juistheid** van de bevindingen.
- In de **rapportage** worden de belangrijkste bevindingen samengevat en de samenhangende risico's toegelicht. In de rapportage is een heat map opgenomen die kan dienen als risicomatrix en kan ondersteunen bij het prioriteren van verbetermaatregelen.
- Parallel doet de auditor een **inschatting van het volwassenheidsniveau**. Aan de hand van concrete aanbevelingen bespreekt de auditor vervolgens de **belangrijkste actiepunten**. Deze vormen de basis voor een deltaplan gericht op het verbeteren van de informatieveiligheid. Het integrale overzicht van de bevindingen komt beschikbaar in een Excel bestand.

Aanpak deltameting

Afhankelijk van de status van de informatieveiligheid, die naar voren komt uit de nulmeting, kan Secura in twee varianten ondersteunen met onafhankelijke delta metingen:

a. **Integrale deltameting**: Dit betekent op een later moment, na de implementatie van alle verbetermaatregelen, vaststellen in hoeverre de verbeteringen effectief zijn voor de criteria in de NEN 7510.
b. **Agile deltameting:** Dit betekent dat in de tijd, op de momenten dat verbetermaatregelen zijn geïmplementeerd, tussentijdse controles plaatsvinden op de daadwerkelijke oplevering. Dit kan plaatsvinden als onderdeel van een projectmatige aanpak van een implementatie.

Gedragslijn Audit 1.0 (1-meting)

De NVZ heeft bestuurlijke afspraken gemaakt met de Autoriteit Persoonsgegevens (AP) voor een '**Gedragslijn Toegangsbeveiliging digitale patiëntendossiers**' (en het bijbehorende auditkader). Onderdeel van deze set van afspraken is dat **aangesloten organisaties zich laten auditen door een gekwalificeerde IT Auditor die bij NOREA is ingeschreven** (RE - Register EDP auditor) om vast te stellen of de minimaal beoogde beveiligingsmaatregelen aanwezig zijn.

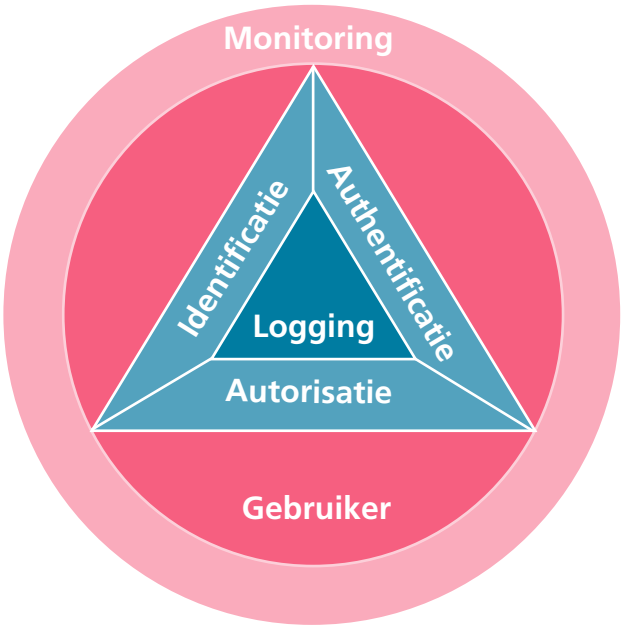
De NVZ heeft dit verder uitgewerkt in acties. **Ten eerste zullen de ziekenhuisorganisaties een self assessment uitvoeren en daarover rapporteren aan de NVZ. Dan bestaat de mogelijkheid verbetermaatregelen te implementeren. Vervolgens dient het management van het ziekenhuis een 'management uiting' te schrijven waarin zij aangeeft in welke mate de organisatie voldoet aan de gestelde eisen.** Deze 'management uiting' is vervolgens het object van onderzoek voor de, met de AP, afgesproken Assurance onderzoeken door een RE. Het betreft een Assurance audit gericht op het geven van een oordeel met redelijke mate van zekerheid volgens de Richtlijn 3000 voor Assurance opdrachten van de NOREA.

Het is aan te bevelen in de nulmeting al de RE-auditor te laten meekijken om helderder te krijgen waar mogelijke aandachtspunten liggen. Natuurlijk wel met de waarborg dat deze RE later de 1-meting nog steeds onafhankelijk kan uitvoeren.

Secura kan deze auditors leveren met ervaring in de gezondheidszorg. In het auditkader zijn vijf normen opgenomen en uitgewerkt, specifiek gericht op de toegangsbeveiliging van digitale patiëntdossiers:

1. **Authenticatie** van toegang: Het uniek identificeerbaar zijn van gebruikers;
2. **Autorisatie**: De logische toegangsbeveiliging tot gegevens en systeem waaronder het toekennen, uitgeven en intrekken van autorisaties;
3. **Logging**: Het betrouwbaar registreren van (geclassificeerde) gebeurtenissen;
4. **Monitoring**: De aanwezigheid en het aantoonbaar gebruik van mechanismes en procedures om (geclassificeerde) gebeurtenissen te monitoren;
5. **Bewustzijn**: Het realiseren van voldoende, en aantoonbare, betrokkenheid van medewerkers bij het realiseren van de beveiliging van de digitale patiëntdossiers.

Een optionele her-audit is mogelijk om na de eventuele verbeteringen alsnog vast te stellen dat de organisatie voldoet. De Gedragslijn Audit 1.0 vindt plaats volgens de Richtlijn 3000 voor Assurance opdrachten en het kwaliteitssysteem van Secura dat voldoet aan de eisen van de NOREA.



Advies & Ondersteuning

Secura heeft uitgebreide ervaring in het inrichten van beveiligingsmaatregelen, alsook in het voorbereiden op NEN 7510 assurance audits dan wel NEN 7510 certificeringen. Uiteraard kan Secura niet adviseren en auditeren voor één organisatie, maar kunnen wij dus wel één van deze rollen voor u vervullen.

Secura levert advies met een integrale benadering van security, waarbij de organisatie, processen, mensen (gedrag) en de techniek allen in beeld zijn. Naast de vele technische assessments op netwerken, applicaties in de zorg levert Secura ook een gericht awareness en gedragsprogramma voor de zorgsector.

Awareness

In het kader van het behalen en behouden van de NEN 7510 accreditering is het van belang om ook te investeren in het veilige gedrag van zorgmedewerkers op de werkvloer. **Secura heeft hiervoor het SAFE programma ontwikkeld dat ziekenhuizen helpt om medewerkers veilig en verantwoord om te laten gaan met de gegevens van patiënten.**

Naast de bestaande awarenesscampagne materialen van de NVZ campagne 'ZEKER', heeft Secura een aanpak ontwikkeld die zich richt op het bevorderen van veilig gedrag. In theorie richt het programma zich daarmee niet alleen op het overdragen van kennis (e-learning), maar betrekt Secura twee andere belangrijke factoren die van invloed zijn op het gedragvan medewerkers: motivatie om veilig gedrag te vertonen en gelegenheid om veilig gedrag te kunnen vertonen. **Secura focust zich met behulp van psychologen op het realiseren van veilig gedrag binnen het ziekenhuis.** Dit geeft de meest effectieve bijdrage aan de kwaliteit van de beveiligingsmaatregelen.

In de praktijk is het programma opgebouwd uit:

- **Awareness nulmeting**
  - Het versturen van één phishingmail
  - Het houden van motivatie & kennistest
  - Het uitvoeren van een site assessment op locatie
- **Basisprogramma voor de hele organisatie**
  - E-learning (met zorgmodules gericht op o.a. EPD)
  - Roadshow
  - Social Engineering
- **Focusgroepen voor specifieke doelgroepen** (verpleegkundigen, HR afdeling)
  - E-learning (met zorgmodule
  - Doelbepaling om gezamenlijke de doelen per doelgroep te bepalen
  - Barriere Assessment om de barrieres die veilig gedrag belemmeren te identificeren
  - Maatwerk interventies om veilig gedrag te realiseren die de barrieres weghalen
- **Awareness deltameting**
  - Deze meting wordt vergeleken met de nulmeting

In samenwerking met Infosequre biedt Secura speciaal voor de zorg een introductieprogramma 'Informatieveiligheid in ziekenhuizen' aan. Deze e-learning module is geaccrediteerd door de beroepsvereniging V & VN. Dankzij de accreditatie kunnen zorgprofessionals die het programma volgen 1 punt verdienen voor het kwaliteitsregister V&V. Daarnaast biedt Secura ook een e-learning module aan gericht op algemene zorginstellingen en een training gericht op onrechtmatige toegang tot het EPD.

Waarom Secura?

Secura is jaren actief in de gezondheidssector en specifiek bij ziekenhuizen op security gerelateerde aandachtsgebieden. Van technische testen tot en met het begeleiden bij of verifiëren van de implementatie van informatieveiligheid. Secura is gecertificeerd voor ISO 27001 en 9001 en voldoet aan de eisen die de NOREA stelt aan het audit kwaliteitssysteem. Binnen Secura werken meerdere RE's intensief samen om een optimale en inhoudelijke bijdrage te leveren aan de security uitdagingen van klanten waaronder ook informatieveiligheid. **Voor ziekenhuisorganisaties heeft Secura een specifieke groep van gecombineerde deskundigheden dat zich richt op de uitdagingen voor ziekenhuisorganisaties en specifieke dienstverlening en tooling ontwikkelt.**

In de uitvoering combineren deze RE's de verschillende deskundigheden die voorhanden zijn binnen Secura waardoor het kwaliteitsniveau van de geleverde dienstverlening op een hoog niveau komt. De RE's van Secura zijn opgenomen in de beperkte lijst van bevoegde auditors die de NVZ samen met de AP heeft opgesteld.

Op basis van de Routekaart ondersteunt Secura klanten met:

1. **Advies en ondersteuning bij de implementatie** van maatregelen gericht op het voldoen aan de gestelde normen, of:
2. **De NEN 7510 Nulmeting** (beperkt voor NVZ eisen, of volledig).
3. **De NVZ Gedragslijn Audit 1.0** (de zogenaamde 1-meting).

Om te zorgen dat de onafhankelijkheid gewaarborgd wordt, zal Secura te allen tijde geen advies **én** assurance dienstverlening leveren aan dezelfde organisatie.

Heeft u interesse in de nulmeting en/of gedragslijn audit of heeft u andere vragen over informatieveiligheid in de zorg: neem contact op.

Wij helpen u graag verder!

Interesse?

Wilt u meer weten over onze services?
Neem vandaag nog contact met ons op!

Volg ons:

+31 88 888 31 00

info@secura.com

secura.com