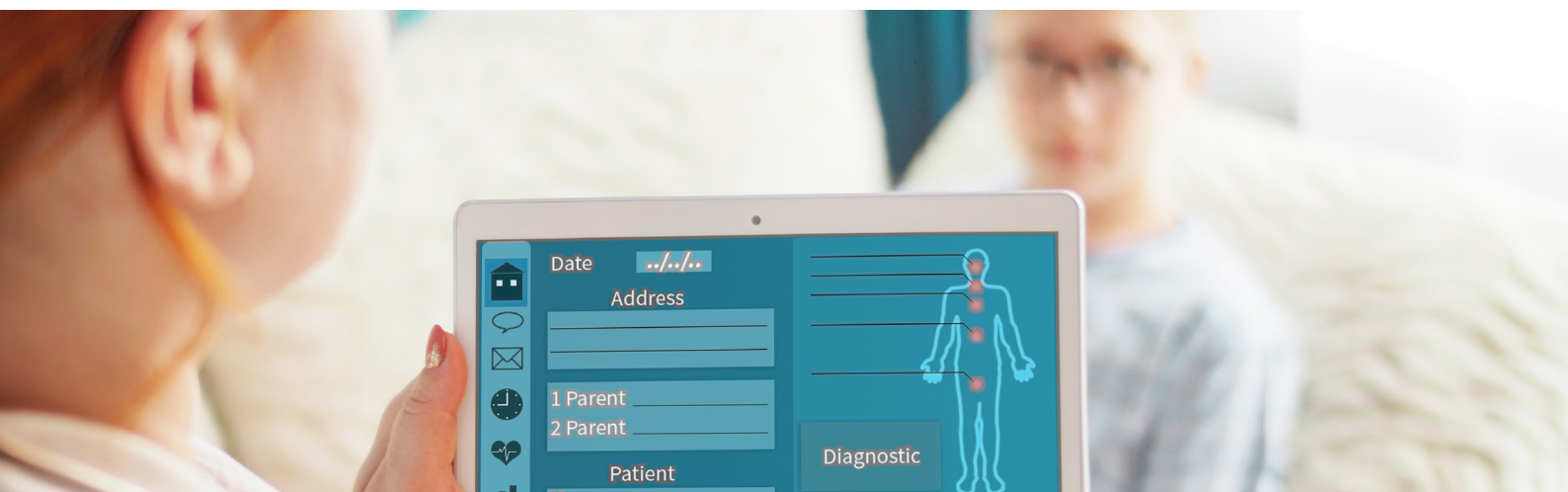




DIGITALISERING VAN DE ZORG

Hoe zorgt u dat u aan alle
beveiligingseisen voldoet?





Digitalisering van de zorg: hoe zorgt u dat u aan alle beveiligingseisen voldoet?

Er verandert veel in de zorg, vooral wanneer we het hebben over informatievoorziening. Zo wordt de patiënt steeds meer een partner voor zorgverleners en heeft hij een andere rol in zijn eigen zorgproces. Hierbij verwacht hij steeds meer onafhankelijk van tijd of plaats gegevens te kunnen inzien of aanpassen.

Daarnaast is het voor zorgprofessionals en -instellingen van belang om op het juiste moment over de juiste informatie te beschikken. Ondanks alle inspanningen die zorginstellingen hiervoor nu al nemen, zet onze regering extra in op de digitalisering van de zorg.

Wetsvoorstel digitalisering zorg

In de zomer van 2020 wordt er een wetsvoorstel gepresenteerd dat zorgverleners en zorginstellingen **verplicht tot digitale dossiervoering en tot elektronische gegevensuitwisseling**. Het gaat de minister voornamelijk om de digitalisering van dossiers, de uitwisseling van gegevens en de regie van de patiënt over het gebruik van zijn gegevens. Daarbij moeten zorginstellingen voldoen aan voorschriften voor taal en techniek. De wettelijke verplichting wordt op twee 'sporen', ingevoerd:

1. Het ene spoor gaat over 'welke' gegevensuitwisselingen we willen digitaliseren.
2. Het tweede spoor heeft betrekking op 'hoe' de digitale gegevensuitwisseling vervolgens moet plaatsvinden.

Privacy en toestemming

Zodra er gevoelige persoonsgegevens worden verwerkt, moet u voldoen aan de AVG/GDPR-wetgeving. Het verwerken van medische informatie is in beginsel verboden. Op dit verbod zijn echter uitzonderingen, bijvoorbeeld wanneer er sprake is van toestemming of wanneer het noodzakelijk is voor de behandeling (behandelovereenkomst). Waar de wet tot onnodig veel oponthoud leidt, wordt in het kader van het bovengenoemde wetsvoorstel bepaald of delen van de betreffende wet aangepast kunnen worden.

Hoe beweegt u mee met deze ontwikkelingen?

Om **zorggegevens veilig en betrouwbaar te kunnen delen** is een duurzaam informatiestelsel nodig. Het Informatieberaad Zorg is opgericht om afspraken, standaarden en voorzieningen te maken voor dit informatiestelsel. Deze afspraken maken zij rondom vier thema's, te weten:

- **Medicijnveiligheid**
Zorgverleners hebben vaak geen compleet beeld van de medicatie van de patiënt, terwijl actuele medicatiegegevens nodig zijn om goede zorg te bieden.
- **Patiënt centraal**
Vanaf januari 2020 bieden zorgverleners burgers de mogelijkheid hun medische gegevens digitaal in te zien.
- **Gestandaardiseerde informatie-uitwisseling**
Zorgverleners dragen vanaf januari 2020 de gegevens die nodig zijn voor goede zorg en behandeling van een patiënt over aan andere bij het zorgproces van die patiënt betrokken zorgverleners. Deze overdracht gebeurt digitaal, gestandaardiseerd, beveiligd en met toestemming van de patiënt.
- **Eenmalig vastleggen van gegevens**
Vanaf 1 januari 2019 gelden er afspraken voor 'eenheid van taal'. Daarmee is de weg vrij om met eenduidig gedefinieerde data te werken aan meer kwaliteit, meer veiligheid en efficiëntere zorg en het vermindert de administratieve belasting voor zorgverleners.

Beveiliging van gegevens

Beveiliging van gegevens is hierbij van het allergrootste belang. Maakt uw instelling gebruik van DigiD, dan heeft Logius- de beheerder van DigiD- maatregelen getroffen voor een basisniveau van beveiliging. Gebruikt uw instelling een andere manier van identificatie of authenticatie? Dan bieden op dit gebied de normen uit het VIPP-programma, aangevuld met de beveiligingsrichtlijnen van NCSC, OWASP, SANS en CIS een goede basis voor uw beveiliging.

DigiD gebruiken binnen uw zorginstelling

Om gebruik te kunnen maken van DigiD voor authenticatie en identificatie binnen uw zorginstelling, moet u voldoen aan een beveiligingsnorm. Deze norm is gebaseerd op de ICT-beveiligingsrichtlijnen voor webapplicaties en is vastgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Om te bepalen of u aan deze norm voldoet, moet u een aantal stappen doorlopen.



DIGID IN DE ZORG IN 6 STAPPEN

Stap 1: toets zelf aan de hand van de richtlijnen

Door eerst na te gaan in hoeverre uw systemen voldoen aan de beveiligingsnorm, krijgt u inzicht in maatregelen die u sowieso moet treffen. Dit voorkomt onnodige verrassingen uit de penetratietest en de audit.

Stap 2: tref maatregelen

Door eerst na te gaan in hoeverre uw systemen voldoen aan de [beveiligingsnorm](#)¹, krijgt u inzicht in maatregelen die u sowieso moet treffen. Dit voorkomt onnodige verrassingen uit de penetratietest en de audit.

Stap 3: voer een penetratietest uit

Schakel een betrouwbare partij in om een penetratietest uit te voeren op uw systemen. Bij deze test wordt er gekeken naar kwetsbaarheden in de beveiliging van uw systemen, om nare verrassingen achteraf te voorkomen.

Stap 4: voer een penetratietest uit

U krijgt na de penetratietest een rapport met bevindingen. Neem maatregelen om de problemen op te lossen.

Stap 5: de audit

Laat een audit uitvoeren door een RE-auditor. Na de audit stelt de auditor een rapportage op een overzicht van de feitelijke bevindingen per maatregel. Per maatregel wordt aangegeven of deze voldoet.

Stap 6: stuur de bevindingen naar Logius

De rapportage over het ICT-beveiligingsassessment DigiD is een gestandaardiseerde rapportage. Het bestuur van uw organisatie stuurt de rapportage, die is ondertekend door de auditor, naar Logius.

Jaarlijks herhalen

De audit voor het gebruik van DigiD moet jaarlijks herhaald worden om er zeker van te zijn dat uw zorginstelling nog steeds aan alle eisen voldoet. Het is daarom belangrijk dat u zich goed informeert over de ontwikkelingen en normen die Logius hanteert.



VIPP-programma

VIPP is het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional. Door dit programma kunnen **zorginstellingen in drie jaar extra stappen zetten om de patiënt toegang te geven tot de eigen medische gegevens**. Digitale toegang, dus via internet. De patiënt kan zo een stuk gemakkelijker informatie van het ziekenhuis raadplegen. Denk aan lab- of andere onderzoeksuitslagen, specialistenbrieven en medicatiegegevens.

Het programma bestaat uit twee delen: gegevensuitwisseling met de patiënt en gegevensuitwisseling tussen professionals en met de patiënt rondom medicatie.

VIPP sluit aan op bestaande landelijke standaarden en draagt bij aan de implementatie daarvan. Dat betekent dat er in dit programma geen nieuwe standaarden worden ontwikkeld, maar dat wordt aangesloten bij landelijke standaarden, waaronder:

- Basis Gegevensset Zorg (BGZ)
- Standaarden medicatieproces
- Standaarden voor uitwisseling met een PGO

Neemt uw instelling deel aan dit programma en wilt u weten of een doelstelling gehaald is, dan vraagt u een eindtoets aan bij een gecertificeerd audit-bureau.

¹ <https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties>

Secura, uw partner voor veilige digitalisering

Secura is gespecialiseerd in digital security en wordt regelmatig ingeschakeld voor beveiligingsadviezen, audits, testen, trainingen en certificeringsdiensten aan onder andere banken, overheden en zorginstellingen.

Securitytesten en penetratietesten

Onderzoek naar de veiligheid van uw IT-omgeving is maatwerk. Voor onze **securitytests** maken wij gebruik van verschillende methoden om de technische beveiligingsrisico's van uw (web) applicaties en IT-infrastructuren te onderzoeken. Hierbij houden wij ook rekening met de zichtbaarheid van uw organisaties en de imagoschade die u door cybercrime zou kunnen oplopen.

Eén van de manieren om kwetsbaarheden in uw IT-omgeving aan het licht te brengen, is de zogenaamde **pentest** (penetratietest). Het doel van een pentest is het binnendringen in systemen (software en/of hardware) met als doel het vinden van zwakke plekken. Vervolgens kunt u maatregelen nemen om de kans te verkleinen dat deze zwakke plekken worden misbruikt.

Secura legt de bevindingen van de security- of pentest vast in **heldere rapportages, een uitgebreide risicoanalyse per bevinding en aanbevelingen op strategisch, tactisch en operationeel niveau**. Dit conform de eisen die gesteld worden zoals voor DigiD.

Audits

Secura verzorgt al jaren de door Logius verplichte jaarlijkse DigiD audits voor haar klanten. Daarnaast leveren wij ook de audits voor het VIPP-programma. Ook helpen wij u graag in de voorbereidende werkzaamheden voor deze audits.

Juist door de inzet van onze security experts kunnen wij ook de technische beveiligingstesten integreren in onze audits. Naast de efficiëntievoordelen die u dit geeft, is het van groot belang dat de beveiliging van uw portalen/applicaties wordt getoetst. De technische testen zijn namelijk geen onderdeel van de VIPP-audit.

Deze diensten kunnen apart, of in combinatie met elkaar worden afgenomen.

Inzicht in uw beveiligingsniveau en voldoen aan eisen

Vindt u het belangrijk om écht inzicht te hebben in het beveiligingsniveau van uw patiëntenportaal of DigiD aansluiting? Kies dan voor Secura. Dan bent u verzekerd van inhoudelijke kennis, vakkundige uitvoering, kwaliteit van de geleverde dienstverlening en pro-actieve begeleiding en ondersteuning in het realiseren van de benodigde beveiliging van uw zorginstelling. Neem vandaag nog contact met ons op via **+31 (0)88 888 31 00** of **info@secura.com**.

Over Secura

Secura is een onafhankelijk, gespecialiseerd kennisbedrijf op het gebied van digitale beveiliging en levert beveiligingsadviezen, audits, testen, trainingen en certificeringsdiensten aan o.a. banken, overheden en zorginstellingen.

Het is onze missie organisaties te ondersteunen met de beste en up-to-date kennis om samen verder te werken aan een heldere en veilige toekomst.

Blijf up-to-date met nieuws, inzichten & advies, events & trainingen en meld u aan voor onze periodieke nieuwsbrief: <https://www.secura.com/nl/subscribe>

Volg ons via:   

*Neem contact op met
info@secura.com of
bezoek [secura.com](https://www.secura.com)
voor meer informatie.*

AANMELDEN

VOOR NIEUWSBRIEF