Onze zorg voor privacybescherming en informatieveiligheid

Connect 4 Care

JUISTE DATA OP DE JUISTE PLEK

Onze zorg voor privacybescherming en informatieveiligheid

1) Het belang van privacybescherming en informatieveiligheid (PB&IV)

In Nederland en Europa neemt de bescherming van privacy en informatie van de zorgafnemer een voorname plek in. Informatie over gezondheid vinden we zodanig privé dat daarvoor een samenstel van strikte wetten en regelgeving is ontwikkeld. Het idee van die wetten en regelgeving is dat de zorgafnemer door middel van het geven van toestemming bepaalt met welke zorgverlener informatie gedeeld mag worden. Strikte (NEN)normeringen moeten ervoor zorgen dat het ook bij de uitvoering niet misgaat.

Van belang is ook dat het Integraal Zorgakkoord (IZA) resultaten verwacht op het gebied van privacybescherming en informatieveiligheid (hierna PB&IV genoemd):

1. ‘Partijen in het IZA werken onder regie van VWS aan het wegnemen van knelpunten om ervoor te zorgen dat elektronische gegevensuitwisseling de standaard wordt. Het belang van privacy en gegevensbescherming wordt altijd meegewogen’ (IZA: p.15).

2. ‘Het veld voldoet voor 2025 aan de wettelijke eisen met betrekking tot de eigen informatieveiligheid en naleving van de geldende NEN-normen en overige wettelijke verplichtingen zoals die uit de wet beveiliging netwerk- en informatiesystemen ten gevolge van de implementatie van de NIB2-richtlijn’ (IZA: p. 95).

Connect4Care heeft een actieve rol als het gaat om privacybescherming en informatieveiligheid. Wij zien erop toe dat leveranciers voldoende maatregelen treffen. Het gaat naast bestaande producten ook om nieuwe toepassingen. Connect4Care is zelf ook gecertificeerd. We voldoen aan de hoogste eisen als het gaat om veiligheid. Daarnaast biedt Connect4Care een leer-werktraject aan dat zorgorganisaties in staat stelt om security officers op te leiden en een informatiebeveiligingssysteem (ISMS) in te richten.

2) Wat wij zelf doen en wat wij van belanghouders verwachten

In onderstaande tabellen laten we je aan de hand van het Nictiz 5-lagenmodel zien welke maatregelen Connect4Care zelf neemt en wat wij van onze afnemers, zorgaanbieders en leveranciers verwachten.

Ten behoeve van de diensten

Nictiz lagenmodel	Connect4Care	Belanghouders
Organisatiebeleid	Connect4Care is NEN 7510 en ISO27001 gecertificeerd. Connect4Care werkt bij voorkeur standaard met het model verwerkersovereenkomst Brancheorganisaties Zorg. Connect4Care heeft een privacyverklaring. Connect4Care is Twiin dienstverlener.	Leveranciers moeten aantoonbaar voldoen aan de NEN 7510 en bij voorkeur gecertificeerd zijn. Met leveranciers worden (sub)verwerkersovereenkomsten afgesloten indien van toepassing. Zorgorganisaties zijn op basis van wetgeving verplicht te voldoen aan de NEN 7510. Connect4Care bevordert de aansluiting op het Twiin Afsprakenstelsel.
Zorgproces	Niet van toepassing: Connect4Care beheert geen zorgprocessen.	Zorgaanbieders zijn zelf verantwoordelijk voor het veilig inrichten van zorgprocessen.
Informatie	Connect4Care beheert een eigen ISMS. We doorlopen de PDCA-cyclus op basis van NEN 7510.	Voldoen aan de NEN 7510 norm.
Applicatie	In de huidige situatie wordt voor identificatie en authenticatie de UZI-pas gebruikt. In sommige situaties wordt gebruik gemaakt van een single sign-on (SSO) vanuit het bronsysteem. Connect4Care biedt veilige e-mail-diensten aan en gebruikt deze ook zelf. Connect4Care beheert loggings-gegevens en informeert patiënt en zorgverlener desgevraagd. Connect4Care heeft geen toegang tot patiëntgegevens, tenzij dat voor de uitoefening van onze taak noodzakelijk is.	Zorgaanbieders zijn zelf verantwoordelijk voor het veilig inrichten van het applicatielandschap. Connect4Care verlangt pentesten van onze leveranciers waar mogelijk en logisch.

IT-infrastructuur	Connect4Care werkt alleen samen met gecertificeerde netwerkpartners die zich verantwoordelijk voelen voor de kwaliteit die zorgnetwerken vereisen. Hierbij staan vertrouwelijkheid, integriteit en beschikbaarheid hoog in het vaandel. Door stakeholders en partners te informeren en te adviseren over de noodzakelijke kwaliteitseisen en mogelijke kwetsbaarheden, werken we gezamenlijk aan een betere en veiligere netwerkomgeving.	Belanghouders zijn verantwoordelijk voor hun data die verstuurd worden over verschillende IT-infrastructuren. Dit houdt in dat zij na moeten gaan of deze data veilig en betrouwbaar verstuurd en ontvangen kunnen worden. De NEN 7510 biedt hierin een handvat om de veiligheid en kwaliteit te garanderen en zo te werken aan een betrouwbare netwerkomgeving.

Ten behoeve van het programma

Nictiz lagenmodel	Connect4Care	Belanghouders
Organisatiebeleid	Wij werken bij voorkeur standaard met het model verwerkersovereenkomst Brancheorganisaties Zorg. Connect4Care is Twiin Dienstverlener.	Leveranciers moeten aantoonbaar voldoen aan de NEN 7510 en bij voorkeur gecertificeerd zijn. Met leveranciers worden (sub)verwerkersovereenkomsten afgesloten indien van toepassing. Zorgorganisaties zijn op basis van wetgeving verplicht te voldoen aan de NEN 7510. Externe projectleiders overhandigen een VOG (Verklaring Omtrent het Gedrag). Connect4Care verwacht aansluiting bij het landelijke Twiin Afsprakenstelsel.
Zorgproces	Niet van toepassing: Connect4Care beheert geen zorgprocessen.	Zorgaanbieders zijn zelf verantwoordelijk voor het veilig inrichten van zorgprocessen.
Informatie	Beheer en onderhoud van het eigen ISMS. Een PDCA-cyclus (Plan Do Check Act) doorlopen vanuit de NEN 7510.	Inrichten van de NEN 7510.

Applicatie	Het samen met leverancier en belanghouders opstellen van een legal framework (juridisch kader). Dit doen we op basis van thema's vanuit de wet- en regelgeving voor gegevensuitwisseling in de zorg waarin we de technische, organisatorische en juridische maatregelen uitwerken. Opstellen van een Data Protection Impact Assessment (DPIA) als de gegevensverwerking een hoog privacyrisico oplevert.	Belanghouders zijn verantwoordelijk voor de maatregelen die beschreven zijn in het legal framework. Opstellen van een DPIA als de gegevensverwerking een hoog privacyrisico oplevert.
IT-infrastructuur	Connect4Care werkt alleen samen met gecertificeerde netwerkpartners die zich verantwoordelijk voelen voor de kwaliteit die zorgnetwerken vereisen.	Belanghouders zijn verantwoordelijk voor hun data die verstuurd worden over verschillende IT-infrastructuren. Dit houdt in dat zij na moeten gaan of deze data veilig en betrouwbaar verstuurd en ontvangen kunnen worden. De NEN 7510 biedt hierin een handvat om de veiligheid en kwaliteit te garanderen en zo te werken aan een betrouwbare netwerkomgeving.

Ten behoeve van kennisopbouw en kennisontwikkeling

Expertisecentrum Privacy & Informatieveiligheid

Een samenwerking van Connect4Care, Sigra en Zorgring voor ondersteuning rondom cyberveiligheid. Het expertisecentrum biedt een netwerk, opleidingen, tools en templates, en detachering van functionarissen gegevensbescherming ten behoeve van de NEN-normen. Het betreft:

- NEN 7510: norm voor informatiebeveiliging in de zorg en ontwikkelen van een Information Security Management System (ISMS);
- NEN 7512: norm voor digitale gegevensuitwisseling;
- NEN 7513: norm voor het patiënt- of cliëntdossier.

Zorgorganisaties in Noord-Holland kunnen tegen betaling deze diensten afnemen.

Security Officer

Connect4Care en Sigra voegen de door hen aangeboden opleidingen samen ten behoeve van een leer-werktraject voor Security Officers. Zorgaanbieders kunnen zo zelf mensen opleiden en ook werken aan een NEN7510-inrichting van hun organisatie.

3) Relevante wet- en regelgeving en normeringen

- AVG: Algemene verordening gegevensbescherming
- BOZ: Standaard Bewerkersovereenkomst Zorg
- EGIZ: Gedragscode Elektronische Gegevensuitwisseling in de zorg
- NEN 7510: norm voor informatiebeveiliging in de zorg en ontwikkelen van ISMS
- NEN 7512: norm voor digitale gegevensuitwisseling
- NEN 7513: norm voor het patiënt- of cliëntdossier
- UAVG: Uitvoeringswet Algemene verordening gegevensbescherming
- Wabvpz: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Wbsn-z: Wet gebruik burgerservicenummer in de zorg
- Wet bescherming Persoonsgegevens
- Wet beveiliging netwerk- en informatiesystemen
- Wet BIG: Wet op de beroepen in de individuele gezondheidszorg
- WGBO: Wet op de geneeskundige behandelovereenkomst

Stichting Connect4Care
Spaarnepoort 5
2134 TM Hoofddorp
023 224 86 13
info@connect4care.nl
connect4care.nl