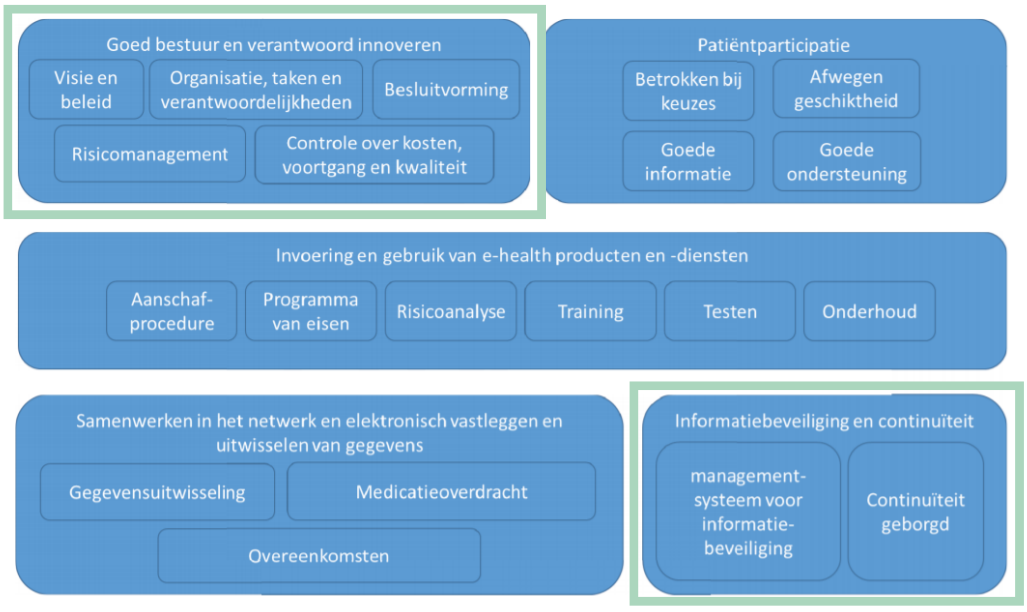
Het toetsingskader e-health IGJ en de NEN7510

Toetsingskaders en normen: wat is als bestuurder goed om te weten? Het op orde hebben van je informatieveiligheid vraagt om het voldoen aan de NEN-norm 7510. Het voldoen aan deze norm is wettelijk verplicht. De IGJ gebruikt de norm in het toetsingskader e-health, waar informatiebeveiliging een onderdeel van is.

Deze norm is niet het enige waar je als zorgorganisatie aan moet voldoen. Er zijn meerdere (NEN) normen en wetten, zoals de Wet digitale overheid, die eisen aan je informatieveiligheid stellen. Maar met het voldoen aan de NEN7510 heb je een grote stap gezet naar bescherming van je digitale gegevens. We geven hieronder een korte uitleg over het toetsingskader e-health van IGJ en over de NEN7510.

Toetsingskader e-health IGJ
De IGJ houdt toezicht op verschillende aspecten in de zorg, zo ook op de juiste randvoorwaarden voor de inzet van e-health door zorgaanbieders. E-health is hier breed bedoeld: de inzet van hedendaagse informatie- en communicatietechnologie (ICT) om de zorg te ondersteunen of te verbeteren. Het IGJ toetsingskader e-health is gebaseerd op wet- en regelgeving en zogeheten 'veldnormen'. Het toetsingskader is opgebouwd rondom 5 thema's:



Bron: Inzet e-health door zorgaanbieders

Als bestuurder heb je een rol in alle aspecten van informatieveiligheid. We lichten er twee uit:

- Goed bestuur en verantwoord innoveren (thema 1): Als bestuurder ben je eindverantwoordelijke en zorg je voor visie en beleid. Je zorgt ervoor dat de informatiebeveiliging belegd en georganiseerd is (waaronder de elementen in de andere blokken van het schema). En dat je aan risicomanagement doet, en dit ook controleert.

- Informatiebeveiliging en continuïteit (thema 5). Als bestuurder ben je eindverantwoordelijke en zorg je ervoor dat je een managementsysteem hebt voor informatiebeveiliging. Daarmee waarborg je continuïteit en houd je toezicht op de uitvoering en effectiviteit van je informatiebeveiligingsbeleid.

Kortom: zorg dat informatieveiligheid een onderdeel is van je managementsysteem en dat je hiervoor een continue PDCA-cyclus inricht en die ook doorloopt. Als bestuurder maak je het informatieveiligheidsbeleid onderdeel van je reguliere, jaarlijkse strategische beleid en controleer je dat dit beleid ook op operationeel niveau geïntegreerd wordt.

Het beleid op operationeel niveau bestaat uit afspraken die nodig zijn, daar waar je eigen organisatie risico loopt. Denk bijvoorbeeld aan beleid voor het gebruik van mobiele apparatuur, voor telewerken, sleutelbeheer, versleuteling van informatie, lege bureaus en afgesloten monitoren. Je stelt de benodigde middelen en mensen beschikbaar voor de uitvoering en communiceert over het belang van informatiebeveiliging. Je ondersteunt je eigen beleid in woord en daad.

Hieronder staan voorbeelden van IGJ rapporten naar aanleiding van een e-health toezichtbezoek aan deze VVT-zorgaanbieders:

- Sensire
- Riethorst Stromenland
- Zonnehuisgroep Amstelland
- Viattence
- AxionContinu
- Frankelandgroep
- Christelijke Zonnehuisgroep IJssel-Vecht
- De Zorgboog
- Zorggroep Ter Weel

NEN7510: verplicht, maar ook een handig hulpmiddel

De NEN7510 geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen om informatie te beveiligen. De NEN 7510 is een algemene norm; NEN 7512 (gegevensuitwisseling) en NEN 7513 (logging) werken deze norm verder uit voor een specifiek aandachtsgebied.

De NEN7510 bestaat uit twee delen: het eerste deel is opgesteld om te voorzien in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. Het tweede deel geeft implementatierichtlijnen hoe de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie te beschermen. Zie de NEN7510 als een routekaart waarbij alle belangrijke elementen van informatieveiligheid voorbij komen, inclusief een lijst aan maatregelen die je kunt treffen. Maar ook hier geldt: bekijk welke maatregelen passen bij jouw eigen organisatie.

Het is verplicht om aan deze NEN-normen te voldoen[1]. Het is echter niet verplicht om je hiervoor te certificeren. Wel moet je aantoonbaar voldoen. Je kunt dit aantonen door bijvoorbeeld een onafhankelijk auditrapport.

De teksten van deze normen zijn vrij beschikbaar.

[1] Volgens het Besluit Elektronische Gegevensverwerking Zorgaanbieders