

### **Wet- en regelgeving en certificeringen**

In Nederland moeten zorginstellingen verplicht werken conform bepaalde normenkaders, zoals de NEN7510. Deze kaders geven een garantie dat informatiebeveiliging een standaard positie heeft in de managementcyclus en dat er middels een risico-gebaseerde aanpak continue verbeterd wordt. Wij doen in dit rapport de aanname dat zorgorganisaties hun interne (werk-) processen en beleid in lijn met dit normenkader hebben ingericht. Voor leveranciers is het hebben van een certificering een pre, hiermee tonen zij aan dat zij dezelfde standaarden hanteren. Daarbij kunnen zij NEN7510 ofwel ISO27001 gecertificeerd zijn. De ISO27001 is een algemene certificering, die niet specifiek voor de zorg is. Daarnaast zijn er een aantal wetten, waarbij de Algemene Verordening Gegevensbescherming de Nederlandse uitleg van de Europese privacy wetgeving is. Deze wet schrijft voor op welke wijze persoonsgegevens verwerkt moeten worden en aan welke richtlijnen je daarvoor moet voldoen.

### **Metadata**

De inhoud van een gesprek leidt tot het verzamelen van data. Daarbij gaat het enerzijds om de inhoud van een gesprek en anderzijds over het verzamelen van de metadata van een gesprek. Dit onderscheid is van belang, omdat in bepaalde gevallen de inhoud van een gesprek wel versleuteld/beschermd is, maar de metadata niet. Metadata zijn alle gegevens over het gesprek, zonder de inhoud. Daarbij kun je denken aan wie er met wie contact heeft, op welk moment, vanaf welk netwerk, IP-adres, op welk tijdstip etc. Deze gegevens lijken onschuldig, maar zijn het alleszins. Wanneer deze gegevens vrijelijk gebruikt mogen worden voor allerlei doeleinden, kunnen deze door commerciële partijen gebruikt worden. Door deze gegevens te combineren met andere datasets kan er ineens gedegen informatie ontstaan over een persoon. Deze metadata moeten daarom ook beschermd zijn en niet vrijelijk gebruikt kunnen worden voor (commerciële) doeleinden.

### **Algemene Verordening Gegevensbescherming (AVG)**

De AVG schrijft voor dat gevoelige informatie in principe binnen de Europese Economische Ruimte (EER) verwerkt moet worden. In deze landen is dezelfde privacywetgeving, de GDPR, in werking. Een uitzondering hierop is wanneer de betreffende organisatie op een andere wijze kan aantonen dat zij alsnog werken volgens de standaarden in de AVG. Er zijn veel zakelijke beeldbel-applicaties beschikbaar die origineel van Amerikaanse afkomst zijn. Voor deze applicaties is het van belang te controleren of zij voldoen aan de Nederlandse wet- en regelgeving en dit af te zetten tegen de Amerikaanse wet- en regelgeving. Het hoeft geen bezwaar te zijn dat een leverancier buiten de EER gevestigd is, mits de juiste maatregelen getroffen zijn.

### **Onderscheid zakelijk en particulier account**

Veel applicaties kennen zowel een zakelijke als een particuliere toepassing. In deze gevallen is het niet altijd mogelijk om een standaard antwoord te geven of de applicatie veilig is. De zakelijke accounts worden betaald en hier worden gerichte afspraken over gemaakt. De particuliere accounts worden over het algemeen niet betaald, waardoor leveranciers anders met de gegevens om kunnen gaan. In de regel kun je (meestal) stellen dat je betaalt met je data wanneer je niet betaalt met geld/financiële middelen. In deze crisistijd gaat dat niet helemaal op, omdat veel grote partijen hun software (tijdelijk) gratis beschikbaar stellen. Hier liggen wel de zakelijke contracten en afspraken aan ten grondslag.

### **Configuratiemogelijkheden**

De meeste applicaties bieden een organisatie ruimte om een aantal zaken zelf te configureren. Dat is in basis heel prettig, maar heeft wel gevolgen voor de snelheid waarmee de applicatie in gebruik genomen kan worden. Daarbij kun je denken aan het bieden van mogelijkheden om een gesprek op te nemen, printscreens te maken etc. Hier moet over nagedacht worden door de organisatie, zodat je weet wat er mogelijk is en waar je data heen gaat.

### **Verwerkersovereenkomst**

Een tool kan op zich zelf veilig zijn, maar vraagt de nodige inrichting om daadwerkelijk compliant te zijn. Een van de onderdelen die daarbij aandacht nodig heeft, is de verwerkersovereenkomst als onderdeel van het contract. Hierin worden afspraken gemaakt wat de verwerker (de leverancier van de tool die je kiest in dit geval) doet met de data die je gebruikt en wat zij daar wel/niet mee mogen doen. Hiermee houdt je als organisatie controle en eigenaarschap over de gegevens en kun je veilig en verantwoord gebruik maken van bepaalde mogelijkheden.

**Er is (nog) geen eenduidig handvat beschikbaar waarmee programma's op veiligheid kunnen worden getoetst. Het kan zijn dat dit handvat wel snel beschikbaar komt, omdat veel zorgverleners hier vragen over hebben.**

**Aan de hand van de volgende vragen kunt u zelf al aandacht besteden aan de veiligheid van een programma:**

- wordt alle communicatie versleuteld (end-to-end encryptie)?;
- is de versleuteling zodanig dat de communicatie onleesbaar is voor de provider?;
- is de beveiliging recentelijk (maximaal twaalf maanden terug) onafhankelijk ge-audit?;
- is het programma specifiek ingericht op de zorg?;
- heeft het programma een [NEN 7510](#) certificaat?;
- heeft het programma een [NEN7512](#) certificaat?;
- heeft het programma een [ISO 27001](#) certificaat?;
- heeft de gebruiker zelf de controle over het opslaan van gesprekken/gegevens?

Niet alle vormen van beeldbellen voldoen aan de veiligheidsnormen van de AVG. In elk geval is contact via WhatsApp, Skype en FaceTime niet voldoende veilig.

**Welke programma's worden wel als veilig beschouwd?**

- [Clickdoc](#) (momenteel gratis toegankelijk voor zorgverleners)
- [E-zorg](#)
- [KPN zorgmessenger](#)
- [Physitrack](#) (videoconsult gratis tot en met 13 april a.s.)
- [Vtell/Vcare](#)
- [Incura](#) (via WeeSeeDo)
- [Zaurus](#)
- Naast bovengenoemde programma's worden o.a. door de KNMG, LHV, NVLF en diverse ICT-websites de volgende programma's aangeraden om te gebruiken:
  - [Gezondheidsmeter PGO+](#)
  - [TinyEYE](#)
  - [Webcamconsult](#) (1 maand gratis proberen)
  - [Facetalk](#)
  - [BeterDichtbij](#)
  - [Quli](#) (drie maanden gratis beschikbaar voor zorgverleners)
  - [Mobiléa](#)
  - [Therapieland](#) (gratis beeldbellen t/m 17 mei a.s.)
  - [Advitronics](#) (gratis videobellen tot 1 september a.s.)
  - [Karify](#)
  - [Viedome](#)
  - [Focuscura](#) (cContact beeldzorg)

Het Nederlands huisartsengenootschap, samen met de landelijke huisartsen vereniging en InEen hebben een mooi overzicht gemaakt over wat 'veilig is voor welk doeleinden' en wat niet. Te vinden na doorklikken op hun pagina: <https://www.nhg.org/coronavirus/hulpmiddelen-voor-uw-praktijk/beeldbellen>.

**Bronnen:**

LHV (Advies over beeldbellen en videoconsult), VVAA, M&I partners (**Rapport** Advies zakelijke beeldbel apps in de zorg **Versie** 1.0 / 27 maart 2020), Eldermans-Geerts, juridisch specialist voor de zorg (Zoom veilig of niet)