

## Security Statement FaceTalk

Versie: 2.1

Jaargang: 2017

### Inleiding

FaceTalk wordt gebruikt voor communicatie in de medische markt waarbij tijdens de videogesprekken vertrouwelijke patiënt gegevens besproken en getoond worden. QConferencing levert de dienst Facetalk en heeft maatregelen genomen om de communicatie op een veilige manier te laten verlopen en heeft haar processen ingericht volgens de ISO27001 norm gericht op informatiebeveiliging. Deze fact sheet geeft een korte opsomming van de maatregelen die QConferencing heeft genomen om de kwaliteit en beveiliging van informatie te borgen en ongeautoriseerd gebruik te voorkomen.

### Eisen vanuit ISO27001 en de Wet Bescherming Persoonsgegevens

In hoofdlijnen komen de maatregelen waarvoor QConferencing de verantwoordelijkheid neemt binnen haar dienst FaceTalk neer op:

1. Een beheerst wijzigingsproces
2. Beschikbaarheid
3. Toegankelijkheid voor geautoriseerde gebruikers
4. Bescherming tegen ongeautoriseerd gebruik
5. Bescherming Persoonsgegevens

### Beheerst wijzigingsproces

FaceTalk is een toepassing welke specifiek ontwikkeld is voor arts-patiënt en arts-arts communicatie. Wensen van gebruikers ten aanzien van verbetering van functionaliteit of uitbreiding van functionaliteit kunnen bij QConferencing aangemeld worden bij de daarvoor verantwoordelijke persoon. Verzoeken worden vastgelegd in het product development document en continue worden nieuwe ontwikkelingen uitgevoerd welke resulteren in nieuwe releases van de FaceTalk software. Nieuwe releases worden eerst vastgesteld, daarna ontwikkeld en getest en tenslotte uitgerold. FaceTalk heeft een online en geïntegreerd logging systeem voor systeem meldingen. Technische storingen worden daarmee automatisch gemeld. Gebruikers kunnen daarnaast vanuit de applicatie vragen stellen of een melding doen van fouten of storingen. Deze worden opgevolgd en gemonitord vanuit een geautomatiseerd ticketing systeem en gecommuniceerd met de betreffende gebruikers. Ticket updates worden via e-mail gecommuniceerd. Waar nodig wordt op andere manieren gecommuniceerd met de gebruiker.

### Beschikbaarheid

De FaceTalk applicatie maakt gebruik van een 2-laags architectuur: een web services laag en de video communicatie services laag. De video communicatie services wordt gehost vanaf dedicated servers. Deze servers worden gemanaged door QConferencing. De video communicatie service is redundant uitgevoerd en draait in een Equinix data center. Het data center is ISO 27001 gecertificeerd. Energie en internet toegang worden bij Equinix afgenomen tegen een afgesproken SLA. De video communicatie apparatuur is redundant uitgevoerd en heeft onderhoudscontracten van de fabrikant met een SLA gericht op 24x7 dienstverlening.

Page 1



De web services laag wordt gehost in het AMS5 data center van Interxion. Dit data center is ook ISO 27001 gecertificeerd.

Voor data opslag in de web services laag wordt gebruik gemaakt van schaalbare EMC<sup>2</sup> storage systemen en software. De server laag is ingericht op basis van voornamelijk HP blade systemen. De onderliggende internet toegang is redundant uitgevoerd en maakt gebruik van oplossingen van Juniper en Fortinet. Door de redundante opzet kan technisch onderhoud worden uitgevoerd zonder onderbreking van de beschikbaarheid.

### **Toegankelijkheid geautoriseerde gebruikers**

Om als gebruiker toegang te krijgen tot de applicatie moeten gebruikersgegevens en een wachtwoord worden ingegeven. Per organisatie kan specifiek wachtwoord management doorgevoerd worden. Voor gastuitnodigingen (patiënten) welke via de e-mail verstuurd worden wordt uitgegaan van de gebruikers identificatie via de e-mail provider.

Voor de toegang tot de admin functionaliteit van de dienst geldt een streng wachtwoord regime en de toegang is beperkt tot een kleine groep medewerkers waarop een strikte controle wordt uitgevoerd.

### **Bescherming tegen ongeautoriseerd gebruik**

Deze bescherming omvat de volgende onderdelen:

1. Fysieke beveiliging van de gebruikte apparatuur door de data centers, onder andere: Fysieke toegangsbeveiligings maatregelen met persoonlijke identificatieplicht, airconditioning, branddetectiesystemen, brandblusinstallaties, camerabeveiliging en inbraakbeveiliging.
2. Beveiliging van informatie tijdens transport. Geautomatiseerde gegevensuitwisseling is beveiligd op basis van HTTPS/SSL in combinatie met beveiligingscertificaten.
3. Beveiliging tegen ongeautoriseerde toegang tot het systeem wordt gecontroleerd door middel van een gebruikersnaam en wachtwoord en het gebruik van unieke in tijd beperkte links voor toegang tot de virtuele vergader ruimtes.
4. Video verbindingen worden opgezet in éénmalige en unieke virtuele kamers. Alleen de genodigde voor een videosessie krijgt de unieke link voor de virtuele kamer via de e-mail. Virtuele kamers zijn maar één dag geldig waardoor hergebruik en toegang buiten die periode niet mogelijk is. De video service laag is videoverbindingen point-to-point encrypted volgens het AES protocol op basis van 256 bits encryptie.
5. Alle diensten componenten worden afgeschermd door strikte firewalls met de bijbehorende beheers regimes.

### **Wet Bescherming Persoonsgegevens**

FaceTalk functioneert met een minimum aan persoonsgegevens. Tijdens de sessie getoonde informatie wordt niet opgeslagen. Er worden geen opnames gemaakt van de videosessies. De Wet Bescherming Persoonsgegevens (WBP) staat het verzamelen van gegevens over personen toe ten behoeve van het eigen primaire proces. Binnen FaceTalk worden de persoonsgegevens in een FaceTalk specifieke database opgeslagen en uitsluitend gebruikt voor het primaire proces. Hergebruik of data uitwisseling met derden is niet mogelijk zonder expliciete schriftelijke toestemming van de gebruiker(s). FaceTalk biedt de mogelijkheid van een geautomatiseerd consent proces waarbij de patiënt eerst consent moet verlenen voordat de videocalls tot stand wordt gebracht. Per organisatie kunnen specifieke afspraken gemaakt worden rond de bewaartermijn van de naw en call log gegevens.

