Security Statement Facetalk 2.0

20 februari 2015

Inleiding
QConferencing beseft dat in haar applicatie FaceTalk gebruikt wordt voor communicatie in de medische markt waarbij tijdens de videogesprekken vertrouwelijke patiënt gegevens besproken en getoond worden. QConferencing heeft maatregelen genomen om de communicatie op een veilige manier te laten verlopen en laat zich leiden door NEN 7510, de norm voor informatiebeveiliging in de Nederlandse zorgsector. Volgens deze norm is een zorginstelling eindverantwoordelijk voor het realiseren van een afgewogen stelsel van veiligheidsmaatregelen. Binnen de FaceTalk applicatie heeft QConferencing hiervoor de vereiste maatregelen genomen.
Deze fact sheet geeft een overzicht van de maatregelen die QConferencing heeft genomen om de kwaliteit en beveiliging van informatie te borgen en ongeautoriseerd gebruik te voorkomen.

Eisen vanuit NEN 7510 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 van tijd tot tijd worden nieuwe ontwikkelingen uitgevoerd welke resulteren in nieuwe releases van de FaceTalk software. Nieuwe releases worden eerst vastgesteld, daarna uitgevoerd 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 een melding doen van vragen, fouten of storingen. Deze worden opgevolgd en gemonitord vanuit een geautomatiseerd ticket aangemaakt en gecommuniceerd met de product ontwikkeling en 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 gebruikt 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 dienstverlening.

De web services laag wordt gehost van het AMS5 data center van Interxion. De processen en het data center zijn ISO 27001, ISO 9001 en NEN 7510 gecertificeerd. ISO 27001 is de internationale standaard voor informatiebeveiliging en -management, gericht op het continue managen, beheren en verbeteren van de informatie beveiliging en bijbehorende risico's. NEN 7510 is de standaard voor beveiliging van medische data. Er wordt uitsluitend gebruik gemaakt van A-merk onderdelen voor alle lagen van de infrastructuur. De ISO 9001 certificering behelst het kwaliteitsmanagement.

Voor data opslag in de web services laag wordt gebruik gemaakt van schaalbare EMC^2 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 gebruikt 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. Het wachtwoord moet voldoen aan de volgende eisen: minimaal acht tekens, waarvan minimaal één cijfer, één hoofdletter, één kleine letter en één bijzonder teken. De toegang wordt geblokkeerd na 5 mislukte pogingen. Het paswoord kan niet hergebruikt worden en elke 6 maanden moet het paswoord gewijzigd worden.
Voor gastuitnodigingen welke via de e-mail verstuurd worden wordt uitgegaan van de gebruikers identificatie via de e-mail provider.

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.

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).