Contact tussen zorgverlener en cliënt

ADVIES ZAKELIJKE BEELDBEL APPS IN DE ZORG

Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | info@mxi.nl | www.mxi.nl

Project
Versie 1.0 / 27 maart 2020
Tessa van Thiel

ICT in perspectief

M&I/Partners/

adviseurs voor management en informatie

INHOUDSOPGAVE

M&I/Partners/

adviseurs voor management en informatie

1 INLEIDING

Tegenwoordig zijn er legio mogelijkheden om op afstand in contact te zijn met elkaar. Verschillende partijen hebben toepassingen die beeldbellen mogelijk maken. In de huidige crisistijd vanwege COVID-19 is dit actueler dan ooit. Beeldbellen maakt het mogelijk dat consulten op afstand plaatsvinden en dat zorgverlener en cliënt niet langer bij elkaar hoeven te komen.
Veel organisaties hebben al een toepassing gekozen om zakelijk beeldbellen te faciliteren. Hierdoor is het al mogelijk om overleg met collega's op afstand te doen. Nu rijst de vraag of deze applicaties ook geschikt zijn voor het contact tussen de zorgverlener en de cliënt. In dit rapport onderzoeken we 7 applicaties. Daarbij beoordelen we primair of deze applicaties voldoen aan de Nederlandse standaarden met betrekking tot informatiebeveiliging en privacy om in te zetten in de zorg.

We starten met een toelichting op een aantal specifieke onderdelen en de uitleg waarom deze zo belangrijk zijn. In hoofdstuk 3 beschrijven we per applicatie onze bevindingen. Tot slot geven we in hoofdstuk 4 een advies welke applicaties het beste in te zetten zijn.
In bijlage 1 is vervolgens een tabel te vinden met nadere informatie per applicatie. Daarin zijn de details terug te vinden waar wij ons oordeel op gebaseerd hebben.

Dit rapport is gebaseerd op informatie die leveranciers beschikbaar gesteld hebben via hun website en/of eventuele resellers. Het onderzoek is in korte tijd uitgevoerd, rekening houdend met de huidige crisis.

2 BEELDBELLEN & INFORMATIEBEVEILIGING EN PRIVACY

In het contact tussen zorgverlener en cliënt worden veel gevoelige zaken besproken. Het is daarom van belang dat de applicatie die hiervoor wordt ingezet ook daadwerkelijk veilig is en voldoet aan de Nederlandse standaarden.

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 Amerikaans 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.

3 RESULTATEN PER APPLICATIE

Wij hebben gekeken naar de volgende applicaties:

- Microsoft Teams
- Zoom
- Microsoft Skype
- Google Hangouts
- Signal
- Whereby
- Microsoft Kaizala.

Microsoft Teams

Microsoft Teams biedt de mogelijkheid om samen te werken in een digitale omgeving. Een van de functionaliteiten die hierbij komt kijken is de mogelijkheid tot beeldbellen. Teams kan zowel met een business account als met een gratis particulier (consumenten) account ingezet worden.
De technische beveiliging van de applicatie is op orde, Teams voldoet aan standaarden als de ISO27001, voldoet aan de AVG door de opslag binnen de EER en heeft aanvullend hierop EU model clauses. Microsoft geeft in hun statements weer dat hun omgeving veilig.

Wanneer de vergadering vanuit de zakelijke Office365-omgeving is opgezet, is dit een veilige omgeving om te kunnen beeldbellen met cliënten. Deze omgeving valt onder de voorwaarden die horen bij de zakelijke omgeving en zijn daarmee voldoende. De consumentenvariant is nadrukkelijk niet geschikt voor cliënt-contact, omdat hier andere voorwaarden aan gesteld worden. Zolang het gesprek onderdeel is van een zakelijke Office365 omgeving, maakt het niet uit of de deelnemer uitgenodigd wordt met een consumenten-account of gastaccount.

Teams biedt veel vrijheid om als organisatie zelf zaken te configureren. Dit is het grote voordeel en de grote uitdaging van Teams. Als organisatie moet je zelf de omgeving dusdanig configureren dat deze compliant is aan de lokale wet- en regelgeving. Wanneer je al bezig bent met deze implementatie en kennis en begrip hebt van de vertaling naar Nederlandse wet- en regelgeving, kun je dit relatief snel goed inrichten. Wanneer je hier nog niets in gedaan hebt, is dit behoorlijk veel werk en is het niet aan te raden om Teams nu op zeer korte termijn in te zetten voor beeldbellen. De configuratie hiervan bevindt zich op verschillende plekken in de admin portal van Office365 en vraagt de nodige tijd en kennis.

Op basis hiervan stellen we dat het gebruik van Teams voor cliënt-contact mogelijk is, mits de juiste stappen gezet zijn in de configuratie. De veiligheid en privacy van cliënten wordt gewaarborgd met een correct inrichting en gebruik.

Zoom

Zoom is primair ontwikkeld voor videoconferencing, waarbij zowel zakelijke klanten als particulieren gebruik kunnen maken van deze toepassing.
Zoom toont middels EU Privacy Shield en EU model clauses aan dat zij werken conform AVG. Ondanks dat Zoom zich op de officiële website profileert als een partij die voldoet aan de Europese privacywetgeving is Zoom de afgelopen weken onder vuur komen te liggen. Zoom is niet transparant over de wijze waarop zij persoonsgegevens verwerkt en welke derden hier toegang toe hebben. Met de informatie die beschikbaar is op de website van Zoom kunnen wij onvoldoende aantonen hoe Zoom zich conformeert aan de AVG.

Zoom biedt de mogelijkheid om met een gratis account (als individu) of een betaald account te werken. In de betaalde, zakelijke omgeving worden de volumes niet beperkt (zoals het aantal minuten dat er gebeld kan worden of de hoeveelheid mensen die deel kunnen nemen) en in de zakelijke omgeving kunnen zaken centraal ingericht worden.
Deze configuratiemogelijkheden maken, als je Zoom wil gebruiken, dat een betaald account aan te raden is. Je hoeft dan niet tijdens ieder gesprek maatregelen te treffen om de privacy en veiligheid van de gegevens te waarborgen, simpelweg omdat je centrale regels kunt invoeren om te voldoen aan wet- en regelgeving en intern beleid.
De cliënt hoeft geen account te hebben en kan deelnemen aan het gesprek op uitnodiging van de zorgverlener.

Waar moet je bijvoorbeeld extra op letten?

- Beeld kan opgenomen worden en chatfiles opgeslagen, maak daar afspraken over en leg daar centraal restricties op;
- De organisator van een vergadering kan zien of je de Zoom app open hebt staan, die instelling staat standaard uit. Zet hier de benodigde restricties op en communiceer hier actief over met de deelnemers als deze feature aan staat;
- Zoom maakt gebruik van rooms (kamers), als host moet je ervoor zorgen dat de juiste deelnemers toegang krijgen tot een room en dus je vergadering. Je kunt deelnemers toelaten aan de hand van een domeinnaam (e-mailadressen) van je organisatie of een wachtwoord;
- Heb je terugkerende vergaderingen, sla dan de instellingen voor die vergaderingen op.

Zorg ervoor dat je bij betaalde accounts het aantal administrators beperkt en organisatorische afspraken maakt over wat zij wel en niet raadplegen.

De betaalde versie van Zoom kan ingezet worden voor beeldbellen met waarbij geen (bijzondere) persoonsgegevens of gevoelige informatie worden gedeeld, mits de juiste configuratie is toegepast. Dit is alleen mogelijk in de betaalde versies van Zoom. Wij raden niet aan om de gratis versie te gebruiken, omdat deze geen mogelijkheden kent om centraal organisatie-instellingen te kiezen. Ieder gesprek is dan afhankelijk van de individuele initiator van het gesprek, wat een risico levert dat er onvoldoende maatregelen getroffen worden.

Op basis van de beschikbare informatie in de privacyverklaring en het gebrek aan transparantie raden wij het gebruik van Zoom in de zorg af. Het gebrek aan informatie maakt dat het op dit moment niet mogelijk is om met voldoende zekerheid te kunnen zeggen dat Zoom een betrouwbare optie is.
Wanneer je als (zorg-)organisatie al gebruik maakt van Zoom en via deze weg ook (bijzondere) persoonsgegevens met elkaar deelt, is het minimaal noodzakelijk om de contractuele afspraken met Zoom te controleren en daar waar nodig aan te scherpen. Let er daarbij op dat er geborgd wordt dat Zoom geen eigenaarschap heeft van de (meta-)data en dat zij de gegevens alleen verwerken voor de doeleinden zoals in het contract beschreven.
Wanneer je nog geen keuze hebt gemaakt, is het aan te raden om voor een ander alternatief te kiezen, waarbij de veiligheid en privacy aantoonbaar geborgd is.

Microsoft Skype

Microsoft Skype kent twee varianten, een zakelijke (skype for business) en een consumenten (skype) mogelijkheid. Skype for business valt onder de zakelijke omgeving van een organisatie en valt daarmee ook onder de afspraken (denk aan een verwerkersovereenkomst) die horen bij een zakelijke omgeving. Skype for business is daarom in te zetten binnen uw organisatie voor contact en overleg[1].
De uitdaging voor contact tussen zorgverlener en cliënt zit in de combinatie van een gesprek tussen iemand met skype for business en de cliënt met een consumenten-skype account.

Microsoft geeft in de privacyverklaring aan dat, in geval van een consumenten-account, er gegevens met derden gedeeld worden vanuit commerciële doeleinden en dat gegevens gedeeld mogen worden met dochterondernemingen. Met deze kennis is het gebruik van een consumenten-skype account, dat veel cliënten zullen hebben of aanmaken, niet voldoende beveiligd en is dit niet geschikt voor contact met een zorgverlener.

Wanneer er een gesprek plaatsvindt tussen een skype for business account en een consumenten-account, valt de informatie over het consumenten account niet onder de zakelijke voorwaarden. Dat betekent dat de inzet van Skype (for business) niet voldoende veilig voor contact tussen zorgverlener en cliënt.

Google hangouts / hangouts meet

Google heeft in de zakelijke G-suite omgeving zowel hangouts (chat app) als hangouts meet (video-vergadering). Gezien de zoektocht naar beeldcontact focussen we in dit onderzoek op hangouts meet. Hangouts meet is niet beschikbaar binnen een consumenten Google account. Daar is wel de optie tot google Duo beschikbaar voor beeldcontact.

---

[1] Aandachtspunt hierbij is dat Microsoft bezig is met een uitfasering van Skype for Business en zelf adviseert om gebruik te maken van Teams. Zoals beschreven onder het kopje Teams biedt dit mogelijkheden voor zorgorganisaties om in contact te zijn en blijven met cliënten.

G-suite (de zakelijke, betaalde variant van google) is een technisch beveiligd platform, dat voldoet aan de verschillende eisen die door de Nederlandse wet- en regelgeving worden voorgeschreven. Ze zijn ISO27001 gecertificeerd en tonen middels EU model clauses compliancy met de Europese privacy wetgeving aan.
G-suite biedt mogelijkheden om een aantal zaken als organisatie te configureren, waaronder de mogelijkheid om gesprekken op te nemen. Afhankelijk van de modules die je afneemt worden de mogelijkheden om gesprekken te doorzoeken groter. Het gebruik van G-suite, en daarmee Hangouts meet, vraagt om een helder beleid en configuratie conform dat beleid.

De gratis consumenten-apps van google voldoet niet aan de eisen die gesteld worden in Nederlandse wet- en regelgeving, Google gebruikt alle verzamelde data onder andere voor commerciële doeleinden.

Het gebruik van Hangouts meet, geïnitieerd vanuit de zakelijke omgeving, voldoet aan de veiligheidseisen, mits goed geconfigureerd. Het gebruik van de zakelijke chat omgeving (hangouts) is ook veilig, mits juist geconfigureerd en in gebruik tussen zakelijke accounts. Het gebruik van hangouts tussen een zakelijke en consumenten-app is onvoldoende beveiligd. Google heeft de ruimte om de gegevens van het consumenten-gesprek te gebruiken voor andere toepassingen.

Hangouts is daarmee niet geschikt voor contact tussen de zorgverlener en de cliënt, omdat beide partijen een account nodig hebben (en de cliënt naar alle waarschijnlijkheid gebruik gaat maken van de gratis versie). Hangouts meet biedt mogelijkheden, mits goed geconfigureerd. Hierbij is nadrukkelijk van belang dat gebruik gemaakt wordt van Hangouts meet als tool voor video-conferencing, waardoor het gesprek onder de zakelijke voorwaarden valt.

Signal

Signal is een relatief eenvoudige chatapp die daarnaast de mogelijkheid biedt om te bellen met beeld. Signal is een open source applicatie, die continue onderhevig is aan peer-reviews. Daarmee is Signal een veilige app, die qua werking vergelijkbaar is met WhatsApp.

Technisch is Signal veilig, er worden voldoende maatregelen genomen om de data te beschermen en zo min mogelijk gegevens op te slaan.
Signal verzamelt zo min mogelijk gegevens en werkt niet samen met derden voor commerciële doeleinden. Vanwege het open source karakter is hier ook geen belang bij.

Signal is een Amerikaanse app, die geen certificeringen heeft waarmee directe compliance aangetoond wordt. De opslag van de beperkte gegevens lijkt in Amerika te zijn, waarbij de opgeslagen gegevens wel versleuteld zijn.

Vanwege de beveiliging en het open source karakter is Signal wel in te zetten voor contact tussen zorgverlener en cliënt. De gegevens over het gesprek worden niet opgeslagen en er is geen commercieel belang om de gegevens te bewaren. Signal is echter wel ontwikkeld als particuliere chat app, dus kan mogelijk in functionaliteiten op lange termijn te kort schieten.

Whereby

Whereby is als videoconferencing tool niet ontwikkeld voor de zorgmarkt. Whereby biedt een gratis variant en een betaalde mogelijkheid om met groepen te beeldbellen.
Whereby heeft geen certificeringen die aantonen dat zij op een goede en veilige wijze met data omgaan. Dit is een minpunt voor het gebruik tussen zorgverlener en cliënt.

De verwerkersovereenkomst staat bij voorbaat gepubliceerd op de website en deze laat ruimte over voor organisaties om afspraken te maken die passen bij het soort data dat er verwerkt wordt. Whereby toont onvoldoende aan dat ze daarbij de nodige maatregelen kunnen treffen die passen bij de gevoelige zorggegevens die in een gesprek tussen zorgverlener en cliënt gedeeld worden.

Whereby toont onvoldoende aan dat ze voldoen aan de richtlijnen die gesteld worden in Nederlandse wet- en regelgeving voor het verwerken van bijzondere persoonsgegevens. Dat wil niet zeggen dat Whereby een onveilige oplossing is.

Het advies is daarom om Whereby in eerste instantie niet te gebruiken voor het contact tussen zorgverlener en cliënt. Het is geen quick win oplossing, die snel passend te maken is voor de zorg. Wanneer je als organisatie al gebruik maakt van Whereby voor andere doeleinden, is het aan te raden om in overleg te treden met de leverancier om samen te bepalen welke maatregelen er getroffen kunnen worden.

Microsoft Kaizala

Microsoft Kaizala kan zowel in een zakelijke omgeving als in een consumentenomgeving toegepast worden. Daarbij is wederom zichtbaar dat de beveiliging en de bescherming van gegevens in de zakelijke omgeving goed geregeld is, via de afspraken die gemaakt zijn tussen de zorgorganisatie en Microsoft.

Bij het gebruik van de consumentenvariant van Kaizala toont Microsoft onvoldoende aan dat de gegevens beschermd worden conform de Nederlandse wet- en regelgeving. Microsoft heeft de ruimte om de meta data in te zetten voor commerciële doeleinden, wat niet past bij gebruik in de zorg.

Het is niet aan te raden om Kaizala in te zetten voor contact tussen zorgverlener en cliënt, omdat de cliënt gebruik maakt van de consumenten-variant. Hierbij gelden dezelfde restricties als bij het gebruik van Microsoft skype. De beschikbare alternatieven van Microsoft bieden meer duidelijkheid en zekerheid over een veilige toepassing van beide kanten.

4 CONCLUSIE EN ADVIES

De verschillende apps die we onderzocht hebben, hebben allemaal hun eigen voor en nadelen. Een aantal conclusies zijn echter te trekken:

- Wanneer er de mogelijkheid is om gratis of betaald gebruik te maken van een dienst, is de betaalde (zakelijke) variant de betere keuzes. In dit geval betaal je met financiële middelen en koop je daarmee de ruimte om zelf de configuratie te doen, passend bij het interne beleid en bij de Nederlandse wet- en regelgeving.
- In bepaalde gevallen is het mogelijk dat de zorgverlener gebruik maakt van een zakelijke toepassing en de cliënt gebruik maakt van de consumenten toepassing. In dat geval is de verbinding en het gesprek onvoldoende beveiligd, omdat de leverancier van het product wel de vrijheid heeft om (meta-)data van het consumenten-deel van het gesprek te gebruiken. De conversatie valt niet automatisch onder de zakelijke voorwaarden, tenzij de ontvangende partij (de cliënt) daar nadrukkelijk toe uitgenodigd wordt. Applicaties die voor consumenten eenvoudig in gebruik zijn en vaak voor andere (particuliere) toepassing al ingezet worden, zijn daarom ongeschikt voor contact tussen zorgverlener en cliënt.
- Deze applicaties zijn niet primair ontwikkeld voor gebruik in de zorg en voor contact tussen zorgverlener en cliënt. De meeste applicaties zijn daar wel geschikt voor te maken, mits de juiste configuratie wordt toegepast. Dat betekent dat de applicatie niet als een quick win in te zetten is.
- Bijna alle genoemde applicatie vragen kennis van de Nederlandse wet- en regelgeving en de kennis en kunde om die te vertalen naar een passende inrichting. Wanneer je als organisatie een van deze organisaties al in gebruikt hebt, kan het een goede optie zijn om de inrichting te reviewen en deze vervolgens in te zetten voor het contact tussen zorgverlener en cliënt. Voor

vrijwel alle applicaties geldt dat het niet aan te raden is om ze nu snel, zonder de benodigde kennis, aan te schaffen en in te zetten.