TELEHEALTH VIDEO APPLICATION SECURITY

Introduction

As the COVID-19 crisis began unfolding in the US, many health systems sought ways to address the challenges caused by rising patient volumes in the emergency departments, hospitals and critical care units as well as the closing of in-person doctor office visits. For many, this meant increasing the use of telehealth video applications for virtual doctor visits and for care of COVID-19 patients in hospitals while limiting staff exposure to the virus.

The move to virtual care became easier when the Office for Civil Rights at the Department of Health and Human Services announced[1] it would "not impose penalties for HIPAA noncompliance against providers leveraging telehealth platforms that may not comply with the privacy regulations during the pandemic." This policy change made it possible for healthcare organizations to consider using commercial or consumer video conferencing applications.

Some healthcare providers have chosen to try commercial-grade video conferencing solutions, with low cost being one of the driving factors. However, there are significant concerns about the ability of these low-cost solutions to meet the security and privacy standards typically required for healthcare related applications.

Security and Privacy Concerns

The issue with trying to adapt a commercial-grade teleconferencing application for a healthcare setting is that many were originally designed for the consumer market, where more focus is placed on affordability and ease-of-use than on security and privacy.

The Fallout from Increased Demand

As more people turned to video-teleconferencing (VTC) platforms to connect with friends, family members, and colleagues during the COVD-19 crisis, reports of video hijacking also began to rise. By the end of March, the FBI had issued a warning[2] after receiving multiple reports of meetings on a popular consumer videoconference platform being disrupted by pornographic and/or hate images and threatening language.

---

[1]Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, HHS.gov, March 30, 2020.

[2]FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI.gov, March 30, 2020

Unfortunately, even as consumer-grade providers rushed to address various security issues surrounding their platforms, new reports of security flaws and privacy violations continued to come forward, including:

- **Videobombing**: the ability to hack into and interrupt an ongoing conference while displaying inappropriate content or behavior. In most cases, the conference was not password protected and used predictable meeting IDs[3].
- **Misleading Encryption Claims**: including the misrepresentation of media encryption levels and extent of encryption capability as it relates to end-to-end encrypted calls. While some providers claimed to offer end-to-end encryption, their version allowed access to encrypted audio and video from meetings. This would not be possible with true end-to-end encryption.
- **Sharing User Data**: some of the most popular consumer-grade solutions were found to have shared user information with third parties[4].
- **Malware**: researchers discovered that software was bundled with malware[5] that affects a PC's processor and graphics card. This malware could enable malicious actors to record sessions and capture text without the knowledge of meeting participants[3].
- **Unsecured Video Calls**: researchers found they could access and download video calls previously recorded to the cloud through an unsecured link[6]. They also discovered that previously recorded user videos could live on in the cloud for hours, even after being deleted by the user.

Establishing Trust

While consumer-grade video conferencing solutions have promised to fix known security flaws, they are essentially asking customers to take their word that the job has been done. Healthcare organizations would be wise to wait for a thorough security audit to be completed by a trusted third party before implementing any consumer-grade teleconferencing solution.

The same due diligence should be applied before considering a so-called "healthcare offering" by these consumer-grade teleconferencing providers. While marketed as a more secure option than the free service, these providers are simply repackaging the same technology and asking healthcare organizations to trust that they meet the HIPAA requirements they are claiming.

[3]Zoom security issues: Zoom buys security company, aims for end-to-end encryption, cnet.com, May 8, 2020
[4]Zoom sued for allegedly sharing users' personal data with Facebook, CBSNews.com, April 1, 2020
[5]Zoom Installers are Being Bundled with Malware, Netsec.news, April 8, 2020
[6]Your Zoom videos could live on in the cloud even after you delete them, cnet.com, April 16, 2020

Finding a Compliant Video Solution

In response to security issues surrounding popular consumer-grade teleconferencing providers, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA) issued cybersecurity guidelines for organizations to consider when implementing VTC[7]. Health systems should thoroughly vet any teleconferencing solution before using, especially if the platform requires attendees to install an application.

When evaluating video conferencing solutions for use in healthcare, consider the following:

- Are video streams encrypted end-to-end and what technologies does the application use for this? Modern standards for web-based video/streaming encryption include AES, HTTPS/TLS, DTLS or SRTP.
- Does the vendor have verifiable, up-to-date security certifications? Has it undergone security and privacy audits by a trusted third party? A trustworthy company will happily provide you with a list of their security credentials upon request.
- Is access to the vendor's systems and data logged, tracked and audited wherever possible? What technologies and security measures are used to secure user accounts?
- Does the vendor use current industry standards and best practices, such as continuous uptime monitoring and monthly security and vulnerability scans, to maintain a secure network?
- Are secure, hardened data centers used to ensure that all core infrastructure is protected and that access to devices and all relevant customer data is restricted and that any access to the data is documented?
- How is privacy and identity protected? Critical data should be segregated so that only authorized users have access to data in its entirety. Conferences should never be recorded, and patient information should not be stored by a videoconferencing service. For added security, sessions should use randomized Consultation/ Meeting IDs that are unique to every call[8].

Benefits of Healthcare-Specific Solutions

Healthcare-designed platforms, such as Caregility UHE, were built to facilitate clinical collaboration and communication around all aspects of patient care. Unlike commercial-grade applications, UHE is always on and available whenever and wherever a provider needs to see and treat the patient. As a healthcare-built solution, UHE can be used for telehealth applications in hospitals such as ad hoc patient check-ins, assessments, consults, and continuous patient monitoring, in emergency departments such as triage and specialty consults, and in outpatient settings such as virtual visits and home-based care.

[7]Cybersecurity Recommendations For Critical Infrastructure Using Video Conferencing, CISA.gov, May 1, 2020
[8]UHE Platform Security Whitepaper, Caregility, May 2020

As a purpose-built, telehealth technology platform, the UHE interface and experience for both the clinician and the patient is consistent across all telehealth programs. UHE is easy to embed, manage, and support, all while ensuring high availability. It was also designed to eliminate the lack of interoperability and serviceability of disparate telemedicine platforms.

Clinicians can also use the platform to perform detailed triage and assessments with the inclusion of high-grade cameras and enhanced audio, to zoom in close to patients and fine tune audio clarity. These are functions most commercial video conferencing apps were not designed to do.

In addition, healthcare-specific solutions may include features such as:

- **Clinician interface**: providing remote audio/visual controls, along with the ability to add other participants into the call, including specialists, interpreters, family, and other care team members.
- **Remote observation**: for continuous observation of multiple patients per clinician on a single screen, which is useful for spot checks and rounding for multiple patients at the same time.
- **Integration with multiple EHRs**: and other clinical workflow software to provide a seamless experience for clinicians.
- **Mobile application**: using mobile devices for clinicians to reach patients in hospitals, EDs, outpatient facilities or at home.

Usability Backed by Security

Of course, it's important that a video conferencing solution be easy to use, especially when it involves patients and their family members. However, ease-of-use should only be considered after an application has been proven to securely manage and protect sensitive healthcare information.

To verify security claims, Caregility hired TRUSTArc, a reputable, third-party privacy consulting company to perform regular audits. Caregility and its UHE platform are ISO97001 certified, CDRP compliant and FIPS compliant end-to-end. Caregility has obtained third-party verification of HIPAA compliance and has undergone annual audits to obtain the US Department of Commerce's Privacy Shield certification.

[9]Coronavirus & Telehealth: COVID-19 Preparedness and Support, Caregility.com, March 12, 2020

Summary

Video conferencing has many applications that can be helpful in a healthcare setting, especially during this time of crisis. While numerous commercial video conferencing options exist, solutions like Caregility UHE™ were purpose-built to enable clinicians to securely communicate with, monitor and care for patients. Ultimately, while affordability and ease-of-use are important, when it comes to the use of video conferencing in a healthcare setting, security and privacy must come first.

Author

Stuart Morris is senior infrastructure architect at Caregility. He can be reached via email at stumorris@caregility.com.

About Caregility

Caregility is a clinical collaboration and communications company focused on enabling the shortest and fastest path of care for patients with the right caregiver and treatment plan. Leveraging our eight years of experience in clinical environments as part of our parent company, Yorktel, our core offering, the UHE Platform, is a purpose-built ecosystem for the entire healthcare continuum.

The UHE Platform provides secure, reliable two-way audio and video communication designed for any device and clinical workflow, in both inpatient and outpatient settings. Today, Caregility supports more than 2 million video sessions and has deployed more than 9,000 access points of care systems across the US. From critical and acute, to urgent and emergent, to post-acute and ambulatory, and to the home, Caregility is helping transform the delivery of patient care everywhere.