Audio-Video Conferencing Risks and Tips for Healthcare Providers

Prepared by:
Kathie McDonald-McClure and Margaret Young Levi
Wyatt Tarrant & Combs LLP

LORMAN®

Published on www.lorman.com - September 2020

LORMAN®

Lorman Education Services is a leading provider of online professional learning, serving individuals and teams seeking training and CE credits. Whether you're looking for professional continuing education or an enterprise-wide learning and development solution, you will find what you need in Lorman's growing library of resources.

Lorman helps professionals meet their needs with more than 100 live training sessions each month and a growing collection of over 13,000 ondemand courses and resources developed by noted industry experts and professionals.

Learn more about Lorman's individual programs, economical All-Access Pass, and Enterprise Packages:

www.lorman.com

Audio-Video Conferencing Risks and Tips for Healthcare Providers

by Margaret Young Levi and Kathie McDonald-McClure

Federal and state governments have relaxed restrictions on telehealth to encourage and empower medical providers to serve patients at home during the novel coronavirus (COVID-19) national public health emergency (PHE). Both medical providers and patients have embraced this new way of connecting due to its convenience and, as a result, the expanded use of telehealth is likely here to stay. The use of audio and video conferencing for patient care, while convenient, risks an unauthorized disclosure of sensitive information if it is used without due regard for whether the connections are secure.

Following expansion by the U.S. Department of Human Health Services' Office for Civil Rights (OCR) and the Centers for Medicare and Medicaid Services (CMS) of federal telehealth services and relaxation of certain requirements during the COVID-19 PHE, Kentucky Medicaid followed suit. See *our previous post* about Kentucky Medicaid's expansion of coverage for telehealth.

OCR Relaxes HIPAA enforcement for telehealth during COVID-19 PHE. OCR, the agency responsible for enforcement of HIPAA, issued guidance on its enforcement discretion with regard to certain telehealth practices under HIPAA. This guidance makes it clear that OCR will not enforce penalties for the use of technology that is not HIPAA compliant, when used in the good faith provision of telehealth services.

Under this Notice, covered health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 PHE.

Obtain patient's consent to telehealth. OCR notes that providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks. Most state laws require that a provider obtain a patient's informed consent to treat via telehealth. During the provider's conversation with the patient to obtain informed consent is the ideal time to make the patient aware of privacy risks of communicating via telehealth.

Select HIPAA-compliant platforms. As an additional protection, providers should research video conferencing platforms and only use ones that are HIPAA compliant. OCR warns that public facing video communication applications, such as Facebook Live, Twitch, TikTok, and others, should not be used in the provision of telehealth. Cyber criminals, aware of the quick turn by U.S. healthcare providers to the use of audio-video conferencing platforms during the COVID-19 PHE, are "hijacking" meetings by taking advantage of security gaps in the use of these platforms.*

Enable the audio-video platform's security features. OCR also advises that "providers should enable all available encryption and privacy modes when using such applications." Providers should familiarize themselves with the features offered by the videoconferencing application, and should consider taking steps to mitigate threats:

- *Ensure your telehealth meeting is not public*. Several widely used platforms, such as WebEx and Zoom, provide features that allow the meeting host to require a meeting password or to use a waiting room feature to control admittance to the communication. For telecommunications that are subject to HIPAA, providers should require a password for admittance to ensure that people cannot access your telehealth meeting without knowing the password. Just as you should be doing for your financial and other sensitive online accounts, use a strong password. Your dog's name or other information that can be readily obtained about you and your family from social media should not be used as any part of your password.
- *Warn patients to confirm the source of any invitation that appears to be from you*. Cybercriminals are taking advantage of the uptick in audio-video telecommunications by sending texts or emails pretending to be an invitation from a trusted source, such as a healthcare provider, associate, friend or family member. Warn your patients to confirm the source of any invitation to join an audio-visual meeting before clicking on a link to what might appear to be your meeting but is actually an invitation from a cyber thief attempting to steal the participant's log-on credentials and password for the online meeting.
- *Do not share a link to a teleconference on an unrestricted, publicly accessible location such as a social media post.* Share it only in an email or text message directly with

the patient with whom you are inviting to your telehealth conference.

- *Manage screen-sharing options*. Both Zoom and WebEx, for example, give the meeting host an option to set the screen-sharing feature to "Host Only."
- *Ensure use of up-to-date applications*. Ensure that you and your patients are using the most updated version of the audio-video meeting application.

HIPAA Business Associates: Determine whether the platform will record and store your meeting. Even though OCR has the discretion not to enforce HIPAA for the use of audio and video conferencing platforms during this public health emergency, other aspects of HIPAA (such as obtaining business associate agreements when necessary) still apply. Medical providers need to determine whether their audio-video telecommunication platform is a HIPAA business associate. A platform is a business associate if it creates, receives, or maintains (e.g., processes and/or stores) electronic protected health information (ePHI)—even if the platform cannot view the ePHI because it is encrypted and it does not have the decryption key. If the platform is only a conduit for the data, and its services are limited to transmission only, then it is not a business associate.

If the platform can record and store a video or audio call with ePHI to the cloud, then it is a business associate and the parties must enter into a business associate agreement (BAA). Most platforms have a standard, non-negotiable BAA form and refuse to sign a provider's form. Some audio-video telecommunication platforms

insist that they're only a conduit yet they sign a BAA, which raises concerns over their understanding of HIPAA. They cannot be both a conduit and a business associate. If the platform you plan to use does not understand this, then they may not understand the HIPAA Security Rule either, raising the question of whether they are truly HIPAA compliant. If after trying to get to the bottom of it, questions remain, look for another platform or seek legal advice.

Conclusion. Delivery of patient care via teleconference and telephone, when other capabilities are unavailable, can go a long way toward easing the burdens on providers (and patients) during the COVID-19 PHE. And there have been indications that the relaxed attitude toward telehealth may continue after the present emergency ends, since both patients and providers appreciate the ability to provide care outside of the office setting. After the PHE ends, providers should be ready to fully comply with HIPAA—so it doesn't hurt to get a head start now and implement common sense precautions to protect patient privacy.

**On April 8, 2020, the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) issued Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors. We encourage readers to review the technical information (which includes screen shots of text messages, emails and fake websites) and extensive mitigation and phishing guidance, as well as tips for defending against online meeting hijacking.*