Video-teleconferencing and Cybersecurity during COVID-19

The Office for Civil Rights (OCR) may waive penalties for dentists who fail to fully comply with HIPAA requirements when communicating with patients via video-teleconferencing during the pandemic providing they act in good faith and do not use public-facing video communication applications.

Dentists using video-teleconferencing to communicate with patients during the COVID-19 public health emergency will not be subject to penalties for HIPAA violations by the Office for Civil Rights (OCR) even if the communications do not fully comply with HIPAA requirements, provided the dentists act in good faith and do not use public-facing video communication applications. See COVID-19 Interim Coding and Billing Interim Guidance. State law restrictions may continue to apply.

The Substance Abuse and Mental Health Services Administration (SAMHSA) has also released guidance on the confidentiality of certain information related to substance use disorder treatment when using video-teleconferencing during the COVID-19 pandemic. See COVID-19 Public Health Emergency Response and 42 CFR Part 2 Guidance.

To help address potential risks associated with video-teleconferencing applications, on April 4 OCR shared an update from the Cybersecurity and Infrastructure Security Agency (CISA) encouraging users to take these steps to help improve video-teleconferencing cybersecurity:

- Ensure meetings are private, either by requiring a password for entry or controlling guest access from a waiting room.
- Consider security requirements when selecting vendors. For example, if end-to-end encryption is necessary, does the vendor offer it?
- Ensure VTC software is up to date. See Understanding Patches and Software Updates.

OCR also shared an FBI warning concerning "hijacking" that may occur when using platforms such as "ZoomBombing" (see ZoomBlog, *A Message to Our Users*, April 1, 2020).

The FBI warning includes these steps to help mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

CISA also recommends the following VTC cybersecurity resources:

- FBI Internet Crime Complaint Center (IC3) Alert: Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments
- Zoom blog on recent cybersecurity measures
- Microsoft Teams security guide

For more information about the FBI warning, see:

- FBI, *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*

For more information about the OCR notification of enforcement discretion, see:

- OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency, March 17, 2020
- OCR Issues Guidance on Telehealth Remote Communications Following Its Notification of Enforcement Discretion, March 20, 2020