Telehealth: Using non-traditional technology for telehealth during COVID-19 Pandemic | March 25, 2020

Health and Human Services' Office of Civil Rights (OCR), the entity responsible for enforcing regulations under HIPAA, stated, effective immediately, it will exercise enforcement discretion and **will not impose penalties for HIPAA violations against covered healthcare providers if patients are served on a good faith basis during the COVID-19 nationwide public health emergency.** OCR has clarified that, during this public health emergency, these technologies can be used for any services, not only those specific to COVID-19. OCR's guidance states, "covered healthcare 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.**" Providers should ensure communication products are non-public facing.

Using one of these technologies should be a last resort, secondary to using traditional telehealth, such as traditional telehealth modalities have healthcare-specific features and security. OCR stresses the importance of using HIPAA-compliant telehealth applications whenever possible from vendors who will enter into Business Association Agreements (BAAs).

DO NOT USE FOR TELEHEALTH

Any video communication applications that are public facing (such as live streaming) should not be used in the provision of telehealth by health care providers. These include the following:

- Facebook Live
- Instagram Live
- Twitch
- TikTok

PERMISSIBLE DURING THIS PUBLIC HEALTH EMERGENCY

Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.

- Apple FaceTime
- Facebook Messenger video chat
- Google Hangouts video
- Skype
- Zoom

MORE SECURE OPTIONS

The list below from OCR includes some vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA.

- Skype for Business
- Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet
- Cisco Webex Meetings / Webex Teams
- Amazon Chime
- GoToMeeting

CONSIDERATIONS FOR USING NON-TRADITIONAL TECHNOLOGIES FOR TELEHEALTH:

DO

Set up service-specific accounts as needed. For example, a dedicated smartphone/iPad or Apple iCloud if FaceTime will be used, dedicated Gmail if Google Hangouts will be used, and/or separate Facebook account if Facebook messenger video will be used.

To create better separation for post-COVID-19 discontinuation of these temporary telehealth services, it may be best to use accounts clearly established just for this purpose. For example, instead of Dr.Joe@examplehc.com, which is the regular email that will be used forever, it may be a new email created just for this, COVID-call@examplehc.com or ABCtele-health@ABChc.com.

Enable two-factor authentication and any other security controls that are reasonable on technologies used for this purpose.

If using Zoom or Skype conferencing, be sure to use a scheduling feature that generates a unique URL whenever possible, this ensures that each patient has their own private link through which to join.

Maintain all other best practices of documentation, communication, and confidentiality.

Manage patient expectations about what is and is not possible connecting through these technologies, including warning them that there may be some level of risk to patient privacy and non-disclosure when using technology.

DO NOT

Conduct these alternative telehealth sessions from the clinician's personal accounts, but *only* from the dedicated cell phone number, Apple iCloud account, or dedicated Gmail account.

Conduct telehealth visits or patient communication in public, on public wifi, or in otherwise unsecure or unencrypted ways. Even with using alternative modalities, it's critical to maintain patient privacy.

Use video conferencing technology that does not have a unique URL for each session, such as a Zoom "Personal Room". Any set up with a static URL (meaning the URL does not change) is potentially problematic, as it runs the risk of someone logging in while still on with another patient, since each does not have a unique URL.

Forget to check with your state, payers, and malpractice insurance provider to understand any specific coverage or reimbursement requirements that may come into play.

Key Information:

- Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, HHS OCR. March 23, 2020.
- Center for Connected Health Policy: Telehealth Coverage Policies in the Time Of Covid-19 to Date, March 19. 2020.
- COVID-19 Resource: Waived Medicare Telehealth Restrictions, Medical Group Management Association. March 17, 2020.

The information contained herein is for informational purpose only and should not be taken as legal, clinical, or reimbursement guidance. The COVID-19 pandemic has created a rapidly changing regulatory environment, so please review linked resources and other relevant information for updates. Check with relevant regulators and payers to confirm up-to-date information.

HITEQ is a national Training and Technical Assistance (TA) Center operated by JSI and Westat. Visit the HITEQ website, www.HITEQcenter.org for more information and resources, as well as to request training or TA. This publication is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $630,000 with 0 percentage financed with nongovernmental sources. The contents are those of the author and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government.