El Camino Health

Telehealth Recommendations & Resources

Version 1.0; April 10, 2020 by James Brummett

Purpose: To provide a summary of recommendations and resources to help physicians utilize conferencing platforms to conduct Telehealth visits with patients. Note that not all recommendations are possible on all platforms and feature names may differ. This document is not all-inclusive of best practices, regulations, or resources. The use of the term "meeting" below is meant to describe the Telehealth visit with a patient.

Recommendations

1. **Require Encryption**
    a. Encryption protects against unauthorized parties from intercepting data in transit. Ensure encryption is enabled by default for all communications.

2. **Use Unique Meeting IDs / Access Codes**
    a. Some platforms utilize Meeting IDs or Access Codes for each meeting, and allow you to reuse these numbers for multiple meetings.
    b. "Limit reuse of access codes; if you've used the same code for a while, you've probably shared it with more people than you can imagine or recall." (Cited Resource #1)

3. **Require Passwords/Passcodes/PINs**
    a. Wherever possible, require a unique password, passcode, or PIN for each meeting.
    b. "Consider using a PIN to prevent someone from crashing your meeting by guessing your URL or meeting ID." (Cited Resource #1)

4. **Use Waiting Rooms**
    a. A waiting room is a virtual holding queue for incoming participants (patients) to wait until the host (physician) manually accepts them into the meeting. This feature helps prevent uninvited participants.
    b. "Use a "green room" or "waiting room" and don't allow the meeting to begin until the host joins." (Cited Resource #1)

5. **Monitor Connected Participants**
    a. "Enable notification when attendees join by playing a tone or announcing names. If this is not an option, make sure the meeting host asks new attendees to identify themselves." (Cited Resource #1)
    b. "If available, use a dashboard to monitor attendees – and identify all generic attendees." (Cited Resource #1)

6. **Disable/Limit Unused Features**
    a. "Disable features you don't need (like chat, file sharing, or screen sharing)." (Cited Resource #1)
    b. If screen sharing is required, "Limit who can share their screen to avoid any unwanted or unexpected images." (Cited Resource #1)

7. **Prepare & Test with Patients**

   a. To help patients get setup and ensure they are prepared for their appointment, it may be necessary to have staff work with patients prior and conduct a test visit.
   b. "All physicians and staff that may be involved in telehealth visits should be trained on the platform and any associated technologies, along with the entire virtual visit process, from sign-on to log-off." (Cited Resource #2)
   c. "Make sure patients know what to expect and how to prepare for their telehealth visits. This includes access to any connected health device or app they should be utilizing, or type of clothing they should wear to make it easier to show wounds, rashes, swelling, or other conditions. They may want to have a trusted assistant on-hand to help hold a camera or flashlight for visual examinations." (Cited Resource #2)

8. **Ensure Quality Network Connectivity**
   a. Poor network connectivity will cause audio and video to lag, be choppy, or fail completely. For both the physician and patient, ensure they have a reliable and high quality network connection. In general this means a wired or wireless connection to a broadband Internet circuit. A cellular data connection from a mobile device is not recommended.
   b. "Make sure patients are aware of minimum requirements for a latency-free experience. Likewise, doctors and staff should make sure they are not experiencing network quality issues." (Cited Resource #2)

9. **Use an Appropriate Solution**
   a. "Covered health care providers that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products. The list below includes some vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA." (Cited Resource #4)
      i. Doxy.me
      ii. Updox
      iii. Zoom for Healthcare
      iv. Skype for Business / Microsoft Teams
      v. VSee
      vi. Google G Suite Hangouts Meet
      vii. Cisco Webex Meetings / Webex Teams
      viii. Amazon Chime
      ix. GoToMeeting
      x. Spruce Health Care Messenger
   b. "Look for a professional telemedicine vendor … that is specialty-centric, which will provide you with a baseline service appropriate for the type of care specific to your practice." (Cited Resource #3)

Cited Resources

1. NIST: Preventing Eavesdropping and Protecting Privacy on Virtual Meetings
   a. https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings

2. Trapollo: 8 Tips to Have Successful Virtual Visits
    a. https://www.trapollo.com/articles/telehealth/8-tips-to-have-successful-virtual-visits
3. Ortholive: Telehealth Etiquette – Conducting the Virtual Visit
    a. https://www.ortholive.com/blog/telehealth-etiquette-conducting-the-virtual-visit
4. HHS: Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency
    a. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Additional Resources

5. HHS: FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency
    a. https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf
6. HIPAA Journal: HIPAA Compliance and COVID-19 Coronavirus
    a. https://www.hipaajournal.com/hipaa-compliance-and-covid-19-coronavirus/
7. AAFP: Operationalizing Virtual Visits During a Public Health Pandemic
    a. https://www.aafp.org/pubs/fpm/issues/2020/0500/p5.html
8. Health IT Security: Telemedicine Privacy, Security Considerations for Providers
    a. https://healthitsecurity.com/news/telemedicine-privacy-security-considerations-for-providers

For further guidance and assistance with Telehealth, as well as other technology needs, it is highly recommended that you engage a qualified and trusted Information Technology professional that focuses on Healthcare.