My Hair Is on Fire:
No Time to Stand up a Telehealth Program in the Middle of a Pandemic!

Susan Clarke, Computer Scientist, HCISSP
Privacy and Security Consultant, Mountain-Pacific Quality Health

Telehealth programs give health care providers an opportunity to deliver services to their patients that might not otherwise be available. They vary significantly in their objectives, size and complexity, and health care organizations will differ in the way they make decisions and in the workflow changes required to put them into action.

Implementing a long-term, sustainable telehealth program takes dedicated resources, money and critical decision-making and may not be a realistic option at this time.

Telehealth Regulations Relaxed for COVID-19

On March 17, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced it will waive penalties for Health Insurance Portability and Accountability Act (HIPAA) that "serve patients in good faith through everyday communications technologies." In response to the COVID-19 public health emergency, providers may now use popular applications for nonpublic-facing communications, meaning applications that provide private video chat, store-and-forward imaging and wireless communications.

OCR noted nonpublic-facing applications typically have certain safeguards to help further secure protected health information (PHI) such as end-to-end encryption, separate logins and passcodes to help limit access and verify participants. To support our partners, Mountain-Pacific Quality Health completed a security analysis to determine some of the controls used by these popular applications and, in some cases, how to enable additional security within the application.

Included in the waiver, providers may not use public-facing applications. Public-facing applications such as TikTok, Facebook Live and Twitch permit the public to access or view the transmission. They also allow live-streaming or the posting of videos onto a public platform. Health care providers who choose to use public-facing applications will not receive the protections under the guidance.

Setting Up for Telehealth

Using consumer-based, "patient friendly" technologies should be a last resort. Preferably, use commercial-based, traditional telehealth such as traditional telehealth modalities that have health care-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). However, if you do find yourself using "patient friendly" technologies, consider the following:

- **Set up service-specific accounts as needed**. For example, if you plan to use FaceTime, dedicate one iPhone/iPad to use. Set up a dedicated Gmail account, if Google Hangouts will be used or a separate Facebook account if you plan to use Facebook Messenger video.

- To create better separation for post-COVID-19 discontinuation of temporary telehealth services, **it may be best to use email accounts clearly established just for this purpose**. For example, if your regular email address is DrEric@wecureyou.com, consider creating and using a new email addresses for COVID-19 telehealth services, e.g., COVIDDocTime@wecureyou.com.

- **Enable two-factor authentication and any other reasonable security controls** 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 each patient has his/her own private link to use to join. If using Skype, enable "private conversation." If using Facebook Messenger, enable "secret conversation" for end-to-end encryption.

- **Find out if and where any data from the telehealth visit is stored** and either ensure encryption or delete the data after the session is over. Make sure to consider any automatic backup that may not be encrypted. Either turn off backup or make sure the backup data are encrypted.

- **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 patients there may be some level of risk to privacy and nondisclosure when using technology.

Avoiding Common Pitfalls

- **Avoid conducting these telehealth sessions from your personal account**. Use a dedicated cell phone number, Apple ID, Skype ID or dedicated Gmail account.

- **Avoid conducting telehealth visits or patient communication in public**, on public Wi-Fi or in otherwise unsecure or unencrypted ways. Even with using consumer-based, "patient friendly" technologies, it is critical to maintain patient privacy.

- **Avoid using 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 you are still on with another patient.

Do not forget to check with your state, payers and malpractice insurance provider to understand any specific coverage or reimbursement requirements that may come into play.

And lastly, check out Mountain-Pacific's new telehealth website, we are here to help you!

This information is brought to you by Mountain-Pacific Quality Health, the Medicare Quality Innovation Network-Quality Improvement Organization (QIN-QIO) for Montana, Wyoming, Alaska, Hawaii and the U.S. Pacific Territories of Guam and American Samoa and the Commonwealth of the Northern Mariana Islands, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. Contents presented do not necessarily reflect CMS policy. 12SOW-MPQHF-AS-CC-20-29