COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 32, Number 38. October 23, 2023

Tips on Telehealth Privacy and Security for Patients

By Nina Youngstrom

Here's a new tip sheet from the HHS Office for Civil Rights.[1] "Telehealth is a wonderful tool that can increase patients' access to health care and improve health care outcomes," said OCR Director Melanie Fontes Rainer in announcing the tip sheet. "Health care providers can support telehealth by helping patients understand privacy and security risks and effective cybersecurity practices so patients are confident that their health information remains private."

Telehealth Privacy and Security Tips for Patients

Using video apps and other technologies for telehealth can create risks to the privacy and security of your health information. This can include when you are accessing telehealth services on a website, through an app or even through a patient portal. Consider these tips to protect and secure your health information.

- **Have your telehealth appointment in a private location.** Find a place away from others (like a private room with a door or your parked car) where you can control who hears or sees your conversation. If you can't find a private place for your appointment, then consider wearing headphones, positioning your computer or mobile device so others can't see your screen, and avoiding using the speakerphone.
- **Turn off any nearby electronic devices that may overhear or record information.** Turn off devices like home security cameras and smart speakers or apps on your phone that respond to your voice, so they don't overhear or record your telehealth appointment.
- **Use a personal computer or mobile device, if possible.** Avoid using a computer, mobile device, or network that is tied to your workplace or a public setting for your telehealth session. Some workplaces and public settings can see what you do when using workplace devices or unsecured, public networks.
- **Install all available security updates on your computer or mobile device.** For most mobile devices, go to the settings icon or tab on your device and turn on the option for automatic updates, or install updates yourself as soon as they're available.
- **Use strong, unique passwords.** Use different passwords for each app, website, computer or mobile device you use for your telehealth appointment to keep others from accessing all of your information if someone discovers your password. If possible, change your passwords regularly.
- **Turn on the lock screen function.** Go to settings and set a short amount of time before your computer or mobile device locks the screen because of inactivity. This prevents someone from getting any of your health information that may be stored on the device unless they have the password.
- **Delete health information on your computer or mobile device when you don't need it anymore.** Removing health information (including photos or videos) from your computer or mobile device helps lower the risk that someone could see your health information if they get your password and can access your computer or

mobile device.

- **Turn on two-step or multi-factor authentication (if it's available and you can use it).** Many apps require you to enter a username and password. Some apps also have an option for multi-factor authentication, which makes it harder for someone else to use the app because they need access to your phone or email. For example, the app may send a code to your phone number or email address that you need to log in to the app. If you need help with multi-factor authentication or can't use it, contact your health care provider to learn what your options are.

- **Use encryption tools when available.** When possible, you should turn on encryption on your phone or mobile device and on any apps that you use to communicate with your health care provider or health plan (like video chat or messaging apps). Encryption is an electronic tool that protects and secures your information by making it unreadable by anyone without the right key or password.

- **Avoid using public Wi-Fi networks and any USB ports at public charging stations.** Public networks (like the ones in coffee shops or airports) may not have security to protect the health information you may want to send using their network. Also, cybercriminals can steal sensitive information by creating fake public Wi-Fi networks that people unknowingly sign onto, or they may use public USB charging ports to install viruses or other malware on your computer or mobile device.

- **Let your provider know if you have any questions about the telehealth appointment or the telehealth technology.** You can ask for help, such as instructions on using the technology or accommodations you need for the telehealth appointment, like a screen reader or closed captioning.

- **If you're suspicious of a link or have any doubts about a link, contact your health care provider right away.** For some telehealth appointments, your provider may send you an email or a link directly to your phone or to your email account. You can always contact your provider to ask if the link they have sent is valid.

- Get more tips to protect your information:

    - **Guidance for Individuals on Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet.** This site has tips to limit how your cell phone, computer, or other mobile device collects and shares your health and other personal information. You can find the guidance at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

    - **Other Telehealth Tips.** This site provides other telehealth privacy tips and resources for patients to help make telehealth sessions more secure. You can find this information at https://telehealth.hhs.gov/patients/telehealth-privacy-for-patients.

    - **Cybersecurity Tips.** This site provides four tips to help keep you safe from cyberattacks and cybercriminals. You can find this site at https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe.