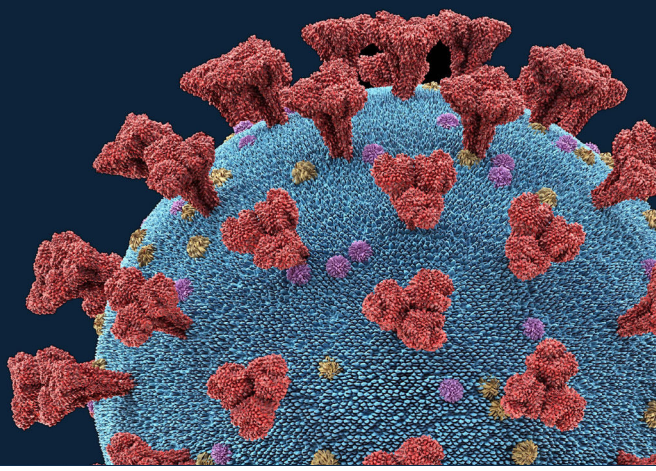
TELEHEALTH PRIVACY AND SECURITY TIPS

FOR HEALTHCARE PROVIDERS AND PATIENTS



In response to social distancing recommendations resulting from the COVID-19 pandemic, healthcare providers are rapidly deploying remote or virtual healthcare services to sustain care for their patients. In many cases, telehealth approaches are new to the patient and the provider and may involve ad hoc solutions to meet communications needs as we contend with a national medical emergency. Maintaining patient privacy remains important. Below are some recommendations from MITRE to maintain patient privacy and security in these challenging times.

FOR HEALTHCARE PROVIDERS

Before Telehealth Sessions

- **Use HIPAA-compliant applications when practical and limit the number of applications used, to help reduce security and privacy risks.** The following link contains recommendations from the Department of Health and Human Services, including applications that are already HIPAA-compliant, options when HIPAA-compliant applications are not workable, and tools to avoid: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.
- **Share updated privacy and security practices with your patients,** using different communications channels such as posting them on your website, or by phone or email when offering appointment reminders. See below for some tips you can provide your patients to safeguard their health information during telehealth sessions.

During Telehealth Sessions

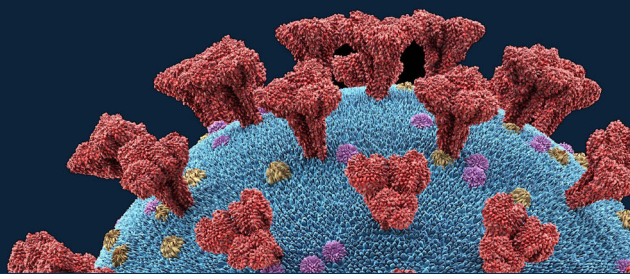
- **Use a private space and limit the number of people who participate in a session.** For providers, this means only permitting personnel directly involved in the patient's care and individuals the patient permits to participate in the session. Secure the room from which you are conducting telehealth sessions (e.g., close the door and post a sign outside the door, indicating unauthorized individuals should not enter while your session is underway). Use headsets to limit audio being heard by others and position screens out of the line of sight of others.
- **Enable all available encryption and privacy modes when using telehealth applications** and notify patients that these third-party applications could potentially introduce privacy risks.
- **Limit the information requested to what is necessary to treat the patient.**
- **Sign out of or close applications and turn off all microphones, cameras, and monitors** once the telehealth session is complete.

Additional Practices

- **Run updates for equipment and applications as soon as they are available,** to take advantage of the latest security capabilities.
- **Secure any notes, written materials, electronic devices, and storage media when not conducting patient sessions.** Avoid saving patient data on personal or shared devices and implement device authentication measures.

TELEHEALTH PRIVACY AND SECURITY TIPS

FOR HEALTHCARE PROVIDERS AND PATIENTS



- **Maintain records of patient interactions and the applications used to conduct each session.** This will be important information for coordinating with vendors to address any concerns regarding removal of records and managing privacy or security breaches.
- **Immediately report a privacy or security breach,** using your existing procedures for doing so if any patient information is lost, accessed, or disclosed inappropriately while scheduling, facilitating, or conducting a telehealth session.

FOR PATIENTS

Before Telehealth Sessions

- **Be aware of updated privacy and security practices from your healthcare provider.** Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.

During Telehealth Sessions

- **Pick a private location.** Hold your telehealth session in a location away from others, such as a room with a door so that you can control who hears your conversation.
- **Secure your device.** Follow your healthcare provider's instructions for securing the device that you use for your telehealth session. Log out of your telehealth session when you are done.
- **Remove unnecessary items.** Before beginning a conversation with your healthcare provider, make sure you remove items that are not needed to discuss your health concerns. Technology devices such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider should be removed to make sure they do not capture potentially sensitive information.
- **Control your background.** Be aware of what will be displayed in the background during a video call and remove any personal information you do not want to share.

MITRE