TELEHEALTH SECURITY AND PRIVACY TIPS FOR PATIENTS

Demand for telehealth services skyrocketed in 2020 in response to social distancing recommendations from the COVID-19 pandemic, and is continuing its ascent into 2021 and beyond. While telehealth is convenient, it can also unexpectedly add cybersecurity risk and impact the privacy of patient information.

Here are some basic tips for improving the security and privacy of your telehealth visits:

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.

ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE. Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.

PICK A PRIVATE LOCATION FOR YOUR VISIT. 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.

BE AWARE OF SCAMS. Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

BE AWARE OF WHAT'S BEHIND YOU. Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.

KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

AVOID USING PUBLIC Wi-Fi NETWORKS FOR YOUR TELEHEALTH APPOINTMENT. Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.

TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION. Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.

LOG OUT OF YOUR TELEHEALTH SESSION WHEN YOU ARE DONE.

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST CYBER