VIRTUAL CARE SECURITY TIPS for patients

Virtual care offers patients convenience, flexibility, and reduced costs. To ensure your information is secure, consider the following safeguards.

**PRACTICE GOOD CYBER HYGIENE**

What is cyber hygiene? Like washing your hands and getting enough sleep, good cyber hygiene is a set of best practices for keeping your digital information healthy and safe.

- **Use strong passwords**
  - A strong password uses 12 or more characters, is unique to each account, and mixes uppercase letters, lowercase letters, and symbols.

- **Use security software on your device**
  - Firewall, antivirus, and anti-malware software help protect your network and devices from harmful activity.

- **Use a secure router**
  - If using a wireless internet connection, check that the router is secure and password-protected with a password set by you.

- **Stay Up to Date**
  - Install current software updates to provide security patches for:
    - Operating systems on phones, tablets, and computers
    - Internet browsers
    - Routers and modems

- **Close the Loop**
  - Sign out of your accounts, close applications, and turn off Bluetooth, microphone, and camera once the virtual care session is complete.

**PRIVACY PLEASE**

When you engage in virtual care, it is critical to know who can see your screen and hear your conversations.

- **Find the right location**
  - Pick a private place for viewing personal health information and virtual visits.

- **Use a secure connection**
  - Do not use public Wi-Fi for virtual care or accessing any sensitive information.

- **Use Bluetooth wisely**
  - Only use Bluetooth connected devices or headphones for virtual care in private settings.

- **Invitation only**
  - Ask your provider to identify anyone else who is in room with them or within earshot. In turn, let your provider know if people in the room with you have permission to be there.

- **Inventory your surroundings**
  - Turn off recording devices and remove anything that displays personal information not necessary for your virtual visit.

- **Think before you click**
  - Email scams are common. If something doesn’t feel right, do not click on it.

**READ UP ON POLICIES**

- From your health care provider
  - Read the updated privacy and security practices from your healthcare provider.

- From your apps and devices
  - Don’t assume all mHealth apps and digital tools are protected by HIPAA regulations.

**TRUST YOUR GUT**

Often our senses alert us to trouble. If something seems off or too good to be true, verify the source before engaging with any email, voicemail, or person.

- **Speak up**
  - Never hesitate to ask your clinic about their safety and security measures or share feedback.

**Disclaimer:** Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.