Virtual care offers many benefits, but it can also increase exposure to cyberthreats. These tips can help keep PHI secure.

**Virtual Care Security Tips for Providers**

**Practice Good Cyber Hygiene**
- Only use a secured Wi-Fi network or a virtual private network (VPN) for your connection.
- Use strong passwords that are unique to each account.
- Use Bluetooth-connected devices and headphones in private settings only.
- Sign off of accounts, close applications, and disable Bluetooth, microphones, and cameras after each virtual care session.
- Keep firewall, antivirus, and anti-malware settings on and up to date.
- Never leave your devices, screens, or papers containing PHI unlocked or unattended.
- Promptly upload patches for your device(s), operating system, browser, and all other software.
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care.

**Follow Security Policy and Regulations**
- Comply with all federal, state, and organizational security rules including protocol for response to a possible data breach.
- Use HIPAA-compliant, encrypted applications and communications.
- Document all virtual patient interactions and note the applications used.
- Promptly report a security breach following your organization’s protocol.
- If cyber insurance is not provided by your practice, obtain a private policy.

**Patient Security and Privacy**
- Share current privacy and security practices and policies with your patients.
- Only permit necessary staff and patient-approved individuals to join the visit.
- Encrypt communications with or about patients.
- Use headphones to prevent others from hearing your conversation.
- Verify you have the patient’s consent to provide virtual care.
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care.
- Introduce any other staff present and explain why they are there.

**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.
- Think before you click. Email scams are common— if something doesn’t feel right, don’t click it.
- Speak up! Check in with your security or IT department if you have questions or concerns.

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