IF YOU CONNECT IT, PROTECT IT

Protecting patients starts with protecting your connected devices. Cyber criminals often gain access to critical and sensitive patient information through connected devices such as phones, computers, wearables, and tablets. Take a look at the tips below to protect your patients and all of your connected devices:



Phone:

Always use a passcode for entry to your cellular device and utilize two-factor authentication when accessing email or network.

Computer:

When connecting your computer to a wireless network, always use a virtual private network (VPN) if possible and protect your data with extra layers of security.



Wearables:

When using wearable devices always ensure they are connected to a secure wifi network or bluetooth connection and disconnect when not using.



Tablets:

Always use a secure wifi network and connect to a virtual private network (VPN) if possible when accessing email and important patient health information.