

# HAVE YOU PERFORMED YOUR CYBERSECURITY CHECKUP?

Take a holistic approach to cyber health. Just as getting regular check-ups is important for your health, it is also important to perform daily cybersecurity “check-ups” to ensure you are being cyber safe and keeping patients safe! Remember the tips from the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients Publication below and perform a head-to-toe cybersecurity check-up!



## HEAD

To keep peace of mind, always ensure you are using strong passwords that protect your organization’s accounts which in turn protects your patient’s data and ensures your healthcare organization’s networks are protected.

**Also, keep your head about you and beware of scamming techniques which can lead to giving out passwords or patient information!**

## HEART

Networks are the heart of every healthcare organization and they hold important patient information and are the key to keeping a healthcare organization running.

**Be careful when using personal devices on your company’s network and ensure you are using the correct protocols when accessing health information.**

## HANDS

Email phishing is the number one way cybercriminals gain access to healthcare organizations, therefore keep your patients safe by resting your hands and taking time to assess emails thoroughly.

**Slow those fingers down and always evaluate emails carefully before clicking on hyperlinks or attachments.**

## FEET

Don’t let cybersecurity failures or breaches trip up your healthcare organization.

**Always ensure you are protecting your IT equipment and if they do grow legs and walk away, ensure to inform your IT professionals that your equipment has been lost or stolen immediately.**

Cyber Safety is Patient Safety which is why performing these cybersecurity checks is an important part of your daily routine. HHS is devoted to partnering with healthcare organizations to advance cybersecurity preparedness across the health sector. We are in this together! HHS, your healthcare organizations, and you are all working together in order to keep our patients safe and make our sector more cyber resilient.