WHAT IS IN YOUR CYBERSECURITY TOOLKIT?

You use medical tools everyday to help keep patients safe and healthy, but did you know that cybersecurity tools are also necessary to keep patients safe?

Include these tools from the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients Publication in your Cybersecurity Toolkit!

KNOW YOUR RANSOMWARE BACKUPS

Just as doctors and nurses always have backup plans for care, it is also important to know your backup plans in case of a cyber-attack. During these events, healthcare facilities are forced to use backup plans to ensure care delivery is not interrupted. To be prepared, ask your IT department or management what your health facility's backup plans are, what your role is, and how best to implement these plans.

IT EQUIPMENT PROTECTION

Doctors protect their medical tools and devices, therefore it is also important to protect your IT and connected equipment. Protecting your authorized IT equipment is important because many cyber criminals gain access to healthcare organizations through lost or stolen equipment. It is also a best practice to encrypt sensitive data on your equipment as a second line of defense.

EMAIL PHISHING AWARENESS

Just as a doctor's stethoscope is used to examine the body, examining your email for potential phishing attempts is equally important. Always remember to stay vigilant and ensure you are checking the sender before taking action. Always double check hyperlinks before clicking.

STRONG PASSWORDS

Strong passwords are a great prescription for fighting cyber attacks. Ensure you are using strong passwords for all of your log-ins both personal and work related.

HHS 405(d)
Aligning Health Care Industry Security Approaches

If you are looking for other cybersecurity best practices, cybersecurity tips, or resources for your healthcare organization check out the 405(d) Program website at 405d.hhs.gov or find us on Social Media @ask405d on Twitter, Instagram, and Facebook!