MITIGATING THE TOP 5 CYBER THREATS

The Nation's critical infrastructure provides the essential services that underpin American society. Ensuring delivery of essential services and functions is important to sustaining the American way of life. Knowing how to safeguard sensitive data within this sector is vital in protecting everyday citizens, which further encourages the idea that:

"CYBER SAFETY IS PATIENT SAFETY.

Email Phishing

Email phishing is an attempt to use email to trick you into giving out personal information or clicking on infected links which give hackers access to all of your patients' data. To be safe, remember that:

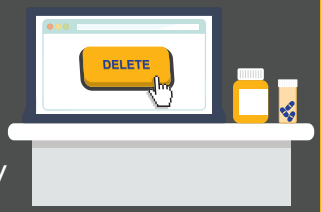
- Files can be hooks; check before you click embedded links
- Websites can be decoys; type in URLs yourself
- Password protected documents can be decoys; verify before opening

Ransomware

A ransomware attack occurs when hackers gain control of data or a computer system and hold it hostage until a ransom is paid. This can put your patients in danger and prevent you from delivering care in a timely fashion.

- Most ransomware attacks begin in email phishing; check the tips above to safeguard your organization's data
- Understand your organization's policies in regard to data back-up and always perform data back-ups regularly

Insider, Accidental, or Intentional Data Loss



Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases.

- Follow your instincts and always report what does not look or feel right to you
- An accidental insider threat is unintentional data loss caused by honest mistakes; notify your IT professional immediately if any data has been lost
- Protect your patients' protected health information and do not give out information unless you have thoroughly identified the requestor's identity

Loss or Theft of Equipment

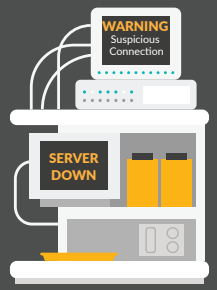
Did you know? Everyday devices such as laptops, smart phones, and USB/thumb drives are often lost or stolen and could end up in the hands of hackers. Make sure that you:

- Never leave your laptop or equipment unattended
- Always encrypt sensitive data that is on your device as a second line of defense
- Notify your supervisor or IT professional immediately if your equipment is lost or stolen

Attacks against Connected Medical Devices

Consider this: Your organization is afflicted by a phishing attack that affects a file server that's connected to multiple heart monitors. The attack gives the hacker complete control to power them off and on as they please.

- To protect your patients, ask your IT professionals about your organization's policies on connected medical devices
- Common vulnerabilities can include legacy or older equipment; always make sure your medical equipment is up-to-date and all new software patches are verified, tested, and installed promptly



HHS 405(d)
Aligning Health Care Industry Security Approaches

Health & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Want More Information or Need to Obtain a Copy of the HICP Publication?
Please visit the 405(d) website at www.phe.gov/405d or email us at CISA405d@hhs.gov