WHAT IS YOUR ORGANIZATION'S CYBER HEALTH REPORT?

Top Five Cybersecurity Threats Facing the Healthcare Industry and Tips on How to Mitigate Them

Email Phishing

Most cybersecurity threats facing your organization come in the form of email phishing. Protect your organization with the following practices:

- Educate your workforce and maintain a training program that focuses on email phishing by implementing regular anti-phishing campaigns with real-time training
- Avoid "free" or "consumer" email systems for your business; such systems are not approved to store, process, or transmit protected health information

Ransomware

Ransomware has the potential to shut down your entire organization and put patients at risk. Don't let hackers hold your data or computer systems hostage; use the following practices:

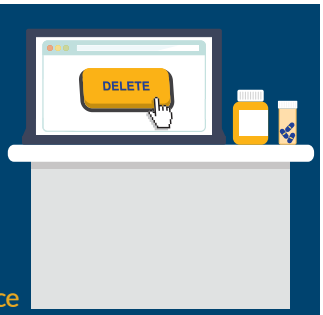
- Instill basic end-point protection controls by removing administrative accounts, keeping end-points patched, and always implementing anti-virus software
- Instill network segmentation by establishing and enforcing network traffic restrictions
- Assess your vulnerability by scheduling vulnerability scans and conducting web application scanning of internet-facing webservers such as web-based patient portals

Loss or Theft of Equipment

Theft of equipment and data is an ever-present and ongoing threat for all organizations. Use the following practices to safeguard your organization:

- Implement policies that address all user interactions with sensitive data and reinforce the consequences of lost, compromised data
- Establish a data classification policy that categorizes data as sensitives, internal use, public use, etc.
- When emailing protected health information, use a secure messaging application such as Direct Secure Messaging

Insider, Accidental, or Intentional Data Loss



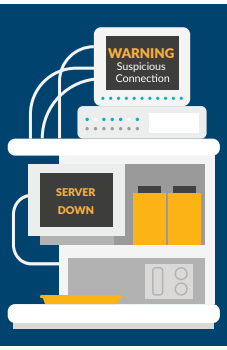
Insider threats exist within every organization. Below are practices used to mitigate this issue:

- Implement policies that address all user interactions with sensitive data and reinforce the consequence of lost, compromised data
- Ensure that cloud-based file storage and sharing systems do not expose sensitive data in an "open sharing" construct without authentication (i.e., do not permit the use of sharing data through a simple URL link)
- Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors

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.

- Configure networks to restrict access between devices that are required to successfully complete work and those that are not. This can limit cyberattacks from spreading across your network.
- Set-up local firewalls. Medical devices should be configured to communicate only with required systems. Unused services and ports should be disabled if they are supported by the manufacturer.



HHS 405(d)
Aligning Health Care Industry Security Approaches

Healthcare & 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.405d.hhs.gov
or email us at CISA405d@hhs.gov