HCIIA Taskforce Bulletin

A Newsletter from the NCHICA Health Care IT/IS Internal Auditors Taskforce

March 2015

Medical devices are like other networked computer systems, they can have vulnerabilities which may cause a security or privacy breach, and potentially have an impact on the safety of patients and device effectiveness. As these medical devices are connected to a facility network, the Internet, or other medical devices, an increase in risk can be expected.

Networked and Implantable Medical Devices

A Networked Medical Device is any network attached non-implanted medical device, e.g., radiology equipment, beds, infusion pumps, monitors, etc. An Implantable Medical Device (IMD) is any patient implanted or patient connected medical device with networking capabilities, e.g., insulin pumps, pacemakers, implantable cardioverter defibrillators and implantable drug pumps.

Risks for these devices are similar to any other technology:

- Default or weak passwords
- Vendor and remote access
- Aged firmware, operating systems, and software
- Insecure or unknown resident data
- Limited logging of access
- Limited or no malicious code protections at the device levels
- Unprotected transmitted and/or device stored data
- Typically forgotten in risk assessments

Common approaches to current device management:

- Informally shared responsibility between clinical engineering and IT departments
- A segmented network for biomedical devices may be deployed
- Currently limited two-way communication paths or device-to-device communication, but rapidly changing
- IMD inventory and procurement typically tracked by departments, not IT or clinical engineering
- Devices often reviewed for clinical, operational and historical patient safety objectives, not privacy and security risks
- Disposal procedures to address resident data not defined
- IT often supports operating system and network attachment, and clinical engineering takes over at the device configuration point.

Risk and Control Considerations

- Are the environments and/or devices monitored based on organization standards for sensitive data?
- Has an assessment of all medical devices been conducted to understand the security and privacy capabilities (i.e., default credentials, logging, password management, default configuration, communication protocols, resident data storage)?
- Does an asset inventory exist to include data fields, communication modality, firmware and operating systems versioning, especially those with remote access and device-to-device access?
- Are software patches and updates monitored and applied as required by policy?
- Are medical devices that cannot conform to the organization's minimal baseline standards identified and isolated on the network?
- Is there a security and privacy review process when considering new equipment for implementation?
- Is remote access and vendor support provided based on company standards for sensitive data?
- Is there a centralized inventory of IMDs to facilitate risk analysis and device management, inclusive of security and privacy concerns?
- Are the disposal procedures based on company standards for sensitive data?

References

- FDA takes steps to strengthen cybersecurity for medical devices
- Wall Street Journal – Citizen Hackers Tinker with Medical Devices
- Computerworld – DHS investigates 24 potentially deadly cyber flaws in medical devices

The NCHICA IT/IS Internal Auditors Taskforce addresses the unique responsibilities of internal auditors who target information technology and information security efforts in healthcare organizations. If you are interested in joining the taskforce, contact allison@nchica.org.