Crowe

Smart decisions. Lasting value.™

# 2019 Crowe Healthcare Virtual Symposium

## Biomedical Devices – A significant risk still not fully understood or managed

February 28, 2019

Robert L. Malarkey, CISSP, CISA

# Housekeeping

- All audio for today's session will be streamed directly to your computer.
- Please submit questions through the Q&A function on your screen.
- To download the presentation, click the resources icon at the lower part of your event console.
- CPE credit
  - Login individually to the session for at least 50 minutes
  - Successfully complete polling questions
- NO CPE credit
  - Fail to successfully complete 3 of 4 polling questions
  - View a recording of this session (CPE is only awarded for live sessions)
- CPE certificate of completion will be e-mailed within two weeks of successfully passing this program

Crowe

Smart decisions. Lasting value.™

# 2019 Crowe Healthcare Virtual Symposium

## Biomedical Devices – A significant risk still not fully understood or managed

February 28, 2019

Robert L. Malarkey, CISSP, CISA

# Today’s speaker

**Robert L. Malarkey, CISSP, CISA**
VP, Healthcare Risk
Crowe Healthcare Risk Consulting

# Agenda

This session will cover the following biomedical device risk topic areas:

- Overview of why this is a significant risk area
- Guidance frameworks and standards
- Biomedical device security
- Biomedical device inventory, tracking and associated challenges
- Governance - who should be managing biomedical devices within an organization
- Takeaway / Summary

# Biomedical Devices – Why is this a significant risk area?

# Biomedical Devices – A Significant Risk Area

**Biomedical device risks are numerous:**

- Patient safety
- HIPAA and other regulatory violations
- Network / system security

**Questions to consider for every healthcare organization:**

- Do you have an accurate inventory of biomedical devices?
- Do you have clearly defined ownership and responsibility for biomedical devices – e.g. Clinical Engineering, IT Security, Procurement, etc?
- Is user access authorized and reviewed for appropriateness?
- Do you have adequate security enabled on devices? Are MDS2 forms available? Are they accurate and validated?
- Do you have policies and procedures specifically governing biomedical devices?

**More devices than ever**

**Uncertain device security**

**Concern for patient safety**

# Biomedical Devices – A Significant Risk Area

- Today's hospitals have **15-17 devices per bed**.—*ECRI*
- Hospitals typically have **300-400% more medical equipment** than IT devices.—*HIMSS*
- 67% of device makers believe it is likely there will be an attack on one of the devices they've built within the next 12 months. —*Ponemon*
- Only about 5% of facilities and 9% of vendors test medical devices annually to make sure they're working correctly and free from security leaks. — *Ponemon*
- The WannaCry attack in summer 2017 crippled 40+ hospitals in the UK affecting CT scanners, x-ray machines, and overall treatment, payment, and operations
- There are approx. 5600 hospitals registered in the United States per the AHA
  - Roughly 500-1000 networked medical devices in a hospital means there are 2.78M to 5.56M medical devices
  - 41% of 158 countries do not have national standards or a recommended list of medical devices for different types of healthcare facilities or for specific procedures. —*World Healthcare Organization*

# Biomedical Devices – A Significant Risk Area

## Notable headlines pertaining to medical device risk:

- CBS National News segment on how pacemakers and insulin pumps can be hacked – November 2018
  https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/
- Prominent healthcare organization knew about pacemaker and defibrillator vulnerabilities, and failed to implement appropriate cybersecurity protections prompting a lawsuit by a third party payer. FDA eventually issued an alert requiring a software patch update for pacemakers to prevent cybersecurity vulnerabilities allowing unauthorized user access to the devices – August 2017
- WannaCry ransomware attack causing loss of access to medical devices, disrupting patient care and productivity – May 2017
  - National Health Service (UK) - At least 6,900 NHS appointments were cancelled as a result of the WannaCry ransomware attack – May 2017

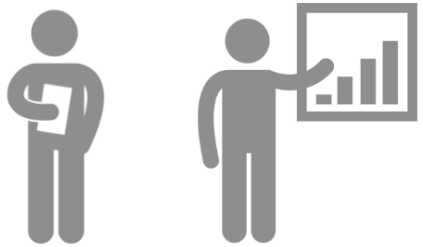
# Why?...for Your Patients

Your priorities…**patients.** When it comes to concerns of security and risk management, the safety of your patients lies at the **heart of every decision** you make. So…

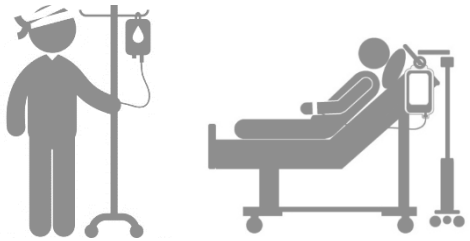
We should all do this…

To take you from this…

To this…

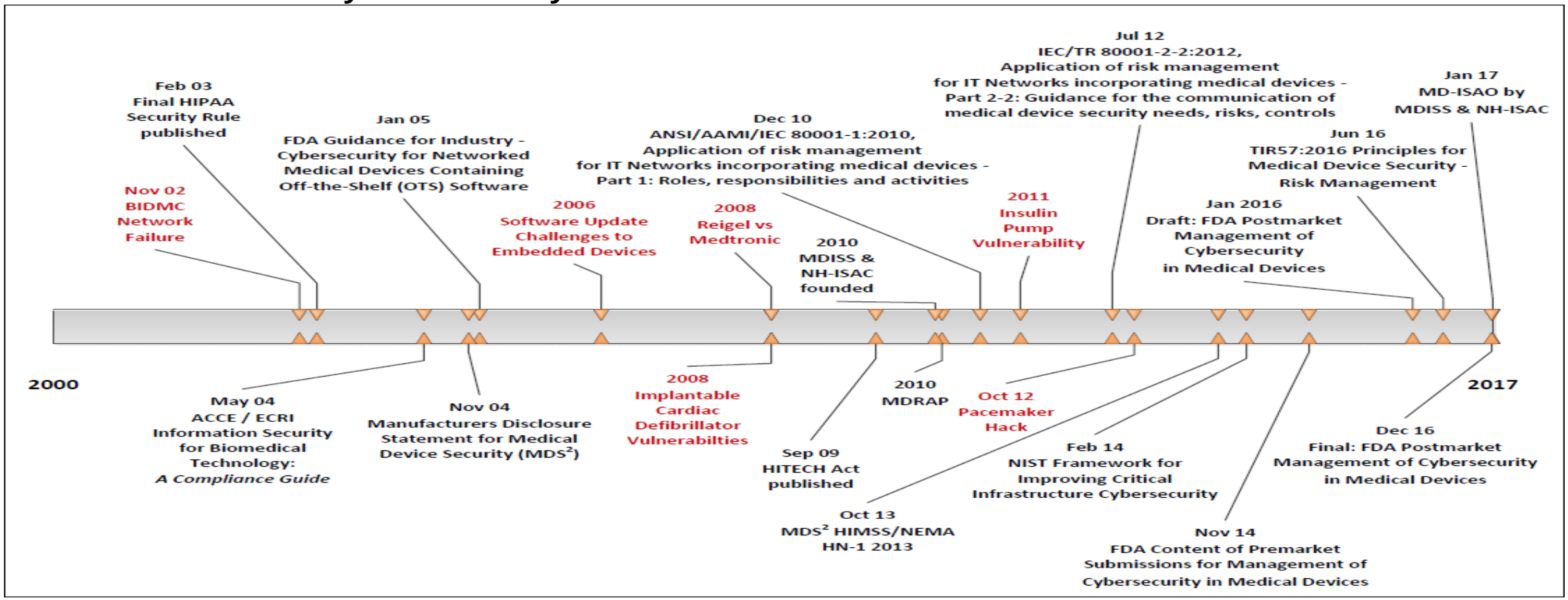


For them…



# Guidance, Frameworks and Standards

# Medical Device Cybersecurity Historical Timeline – Jan 2000 To Jan 2019




1

August 2018 – NIST SP 1800-8A – Securing Wireless Infusion Pumps
Oct 2018 – FDA - Premarket Submissions for Management of Cybersecurity in Medical Devices
Oct 2018 – FDA MITRE - Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
Jan 2019 – The HSCC – Medical Device Joint Security Plan



1. https://mdviper.org/backgroundreferences/historical-timeline/

# Commit to a Framework

# Food And Drug Administration

- Food and Drug Administration (FDA) Post Market Management of Cybersecurity in Medical Devices – Final Guidance
  - Targeted at manufacturers, not healthcare providers

**Regulatory Gaps**

- FDA guidance is not mandatory, and focuses on device safety from a physical patient health perspective

- FDA cybersecurity incident reporting is only required when the cybersecurity incident is related to the death or injury of a patient – meaning known cybersecurity events could be unreported

- And….Side note……per the OIG: FDA's post-market cybersecurity policies and procedures are lacking

# HIPAA

- Health Insurance Portability and Accountability Act (HIPAA) - Security Rule and Privacy Rule
  - Security Rule: Administrative, Technical and Physical Safeguards, include the Risk Analysis requirement
  - Data Access and Disclosure Safeguards (Privacy Rule)


**Regulatory Gaps**

- HIPAA regulations do not specifically call out biomed device requirements.
  - Devices that interact with ePHI are to be held to HIPAA Requirements
  - No standardized interpretation of HIPAA Requirements to device specifications

- What you and your HIPAA Team need to be aware
  - Your organization’s annual risk analysis (§ 164.308(a)(1)(ii)(A)) has to include biomedical devices

# HIPAA

- The Office for Civil Rights (OCR) HIPAA audits will include focus on networked medical devices
- The Office of Inspector General (OIG) includes biomedical device security their Workplan (continuously updated monthly)
- $850,000 fine and Corrective Action Plan due to unmanaged workstations associated with a CT Scanner: https://www.hhs.gov/sites/default/files/lahey.pdf

# Other Guidance And Frameworks

- National Institute of Standards and Technology (NIST) Cybersecurity Framework and SP 800-53
  - Cybersecurity Framework cross references with other controls such as ISO, SP 800-53, COBIT
  - SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
  - Maps to ISO/IEC controls

- International Organization for Standardization (ISO) / American National Standards Institute (ANSI) / International Electrotechnical Commission (IEC) 80001
  - Application of risk management for IT networks incorporating medical devices

- Healthcare & Public Health Sector Coordinating Councils
  - Medical Device and Health IT Joint Security Plan

NIST National Institute of Standards and Technology U.S. Department of Commerce

ISO International Organization for Standardization

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

Healthcare & Public Health Sector Coordinating Councils PUBLIC PRIVATE PARTNERSHIP

# Manufacturer Disclosure Statement For Medical Device Security (MDS2)

Developed by National Electrical Manufacturers Association (NEMA) and Healthcare Information and Management Systems Society (HIMSS)

- Manufacturers fill out an MDS2 for their devices
- Questions covering security features on the device

## Information Gaps

- Voluntary
- Not usually publicly available, must be requested by purchasing entity

Manufacturer Disclosure Statement for Medical Device Security – MDS²

| | | | |
|---|---|---|---|
| Device Category | Manufacturer: Carestream Health Inc. | Document ID: DH5015 | Document Release Date: 8/4/2017 |
| Device Model: DirectView DR7500 | Software Revision: 6.0 | Software Release Date: April 2008 | |

| | | | |
|---|---|---|---|
| Manufacturer Representative Contact Information: | Name: Technical Support | Title: N/A | Department: USG Service |
| | Company Name: Carestream Health Inc. | Telephone #: 1-800-328-2910 | e-mail: |

ASSESSMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)

| | | | |
|---|---|---|---|
| 1. | Can this device transmit or maintain electronic Protected Health Information (ePHI)? | Yes | |
| 2. | Types of ePHI data elements that can be maintained by the device: | | |
| a. | Demographic (e.g., name, address, location, unique identification number)? | Yes | |
| b. | Medical record (e.g., medical record #, account #, test or treatment date, device identification number)? | Yes | |
| c. | Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)? | Yes | |
| d. | Open, unstructured text entered by device user/operator? | Yes | |
| 3. | Maintaining ePHI. Can the device: | | |
| a. | Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)? | Yes | |
| b. | Store ePHI persistently on local media? | Yes | |
| c. | Import/export ePHI with other systems? | Yes | |
| 4. | Mechanisms used for the transmitting, importing/exporting of ePHI: Can the device: | | |
| a. | Display ePHI (e.g., video display)? | Yes | |
| b. | Generate hardcopy reports or images containing ePHI? | Yes | |
| c. | Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)? | Yes | |
| d. | Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)? | No | |
| e. | Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)? | Yes | |
| f. | Transmit/receive ePHI via an integrated wireless connection (e.g., WiFi, Bluetooth, infrared)? | No | |
| g. | Other | N/A | |

ADMINISTRATIVE SAFEGUARDS

| | | | | |
|---|---|---|---|---|
| 5. | Does manufacturer offer operator and technical support training or documentation on device security features? | Yes | | 1 |
| 6. | What underlying operating system(s) (including version number) are used by the device? | Microsoft Windows 2000 SP4 | | |

PHYSICAL SAFEGUARDS

| | | | | |
|---|---|---|---|---|
| 7. | Are all device components maintaining ePHI (other than removable media) physically secure (i.e., cannot remove without tools)? | Yes | | 2,3,4 |
| 8. | Does the device have an integral data backup capability (i.e., backup onto removable media such as tape, disk)? | Yes | | 5 |
| 9. | Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? | Yes | | 6 |

TECHNICAL SAFEGUARDS

| | | | | |
|---|---|---|---|---|
| 10. | Can software or hardware not authorized by the device manufacturer be installed on the device? | Yes | | |
| 11. | Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)? | Yes | | |
| a. | Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)? | Yes | | |
| b. | Can the device log provide an audit trail of remote-service activity? | Yes | | |
| c. | Can security patches or other software be installed remotely? | Yes | | |
| 12. | Level of owner's security or service access to device operating system: Can the device owner/operator: | | | |
| a. | Apply device manufacturer-validated security patches? | Yes | | |
| b. | Install or update anti-virus software? | No | | |
| c. | Update virus definitions on manufacturer-installed anti-virus software? | No | | |
| d. | Obtain administrative privileges (e.g., access operating system or application via local root or admin account)? | Yes | | |
| 13. | Does the device support user/operator specific ID and password? | Yes | | |
| 14. | Are access sessions terminated after a predetermined length of inactivity (e.g., auto-logoff)? | Yes | | |
| 15. | Events recorded in device audit log (e.g., user, date/time, action taken): Can the audit log record: | | | |
| a. | Login and logout by users/operators? | Yes | | |
| b. | Viewing of ePHI? | Yes | | |
| c. | Creation, modification or deletion of ePHI? | Yes | | |
| d. | Import/export or transmission/receipt of ePHI? | Yes | | |
| 16. | Does the device incorporate an emergency access ("break-glass") feature that logs each instance of use? | No | | |
| 17. | Can the device maintain ePHI (e.g., by internal battery) during power service interruptions? | Yes | | |
| 18. | Controls when exchanging ePHI with other devices: | | | |
| a. | Transmitted only via a physically secure connection (e.g., dedicated cable)? | No | | |
| b. | Encrypted prior to transmission via a network or removable media? | No | | |
| c. | Restricted to a fixed list of network addresses (i.e., host-based access control list)? | Yes | | 7 |
| 19. | Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology? | Yes | | |

¹ Requirement per DICOM's Universal Medical Device Nomenclature System (UMDNS)

Carestream Health Inc. MDS² v 1.0 – DirectView DR7500 ©2001, HIMSS. All rights reserved.

# The MDS2 – Good Starting Point; May Not Be All Inclusive

- Great point to ***START***
  - Need to obtain upfront during procurement
  - Evaluate details and understand implications

- Need a reliable inventory to apply against

- Need good governance program to inform all key parties and empower them to act

  - Clinical Engineering and Security – configuration matters
  - Third-party risk / legal / procurement – are settings/configurations acceptable? Can organization mitigate or need to go to manufacturer? Does business understand risk assumed if unable to mitigate? Documented?

- What else are you using along with MDS2 forms?
  - MDRAP is a good start if you have nothing else to help assess and understand the security of your medical devices
  - Can your medical device lifecycle management and maintenance third party help?

# Polling Question #1

**What guidance does your company primarily use for biomedical device risk assessment and management?**

a. HIPAA Privacy and Security Rules
b. NIST Cybersecurity Framework
c. FDA Cybersecurity Guidance
d. ISO / ANSI / IEC Standards
e. Company standards (customized)

# Biomedical Device Security

# Biomedical Devices Security – Common Controls and Gaps

- What can a healthcare provider do vs. the device manufacturer
- Network segmentation – correct starting point?
- Common Security Controls
  - Log-in / log out
  - Can data be removed from the device
  - User access – does the device allow different levels of access, different roles and privileges
  - Are you able to configure the security settings
  - Can you remove ePHI data and/or de-identify it
  - Logging and monitoring – can you tell if data has been accessed, modified, deleted
  - Can data be backed up, can devices be tested during disaster recovery exercises
  - Is anti-virus software installed, can it easily be updated
  - Are devices current on patches
  - Physically secured
  - Hardening measures to prevent cyber attacks and malware
  - Third party security – during updates, maintenance
  - Data transmission security
  - Remote access

# Biomedical Devices Security – Common Controls and Gaps - Continued

- Common medical device security vulnerabilities
  - Lack of user access provisioning and security controls – terminated users, admin, non-compliant passwords
  - Not integrated with Active Directory
  - Outdated operating systems, non-supported, proprietary – at the mercy of the OEM
  - No encryption --- means ePHI is not encrypted
  - Cannot perform a vulnerability scan or a penetration test – too risky

- Profiling devices

- Security responsibility – Is this only the responsibility of the Information Security group?

# Polling Question #2

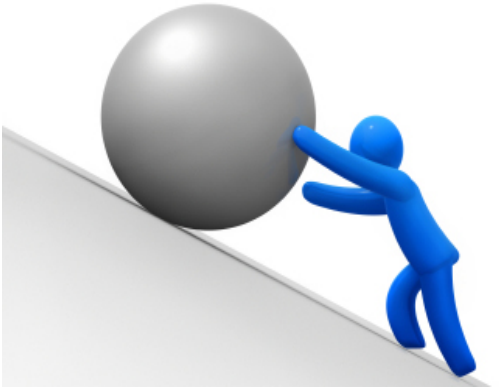
**Who is responsible for biomedical device *security* within your organizations? (click all that apply)**

a. Information Services / Information Technology
b. Clinical Engineering
c. Procurement
d. Outsourced to a Third-Party (vendor/contractor)
e. Dedicated committee
f. Not well defined

# Biomedical Device Inventory, Tracking and Associated Challenges

# Biomedical Device Inventory

- Questions a healthcare organization should ask:
  - Did all devices go through a consistent procurement process?
  - Is all device information documented and maintained in a central repository?
  - How are devices procured, assessed, remediated/mitigated, managed and disposed of across the organization's footprint?
  - What inventory strategy best suits your organization, and what is your risk tolerance?
  - Can devices be logically accounted for --- comprehensively?
  - Do you employ third parties to maintain a comprehensive inventory?
  - If you were audited, do you feel confident that the full inventory is documented and maintained?



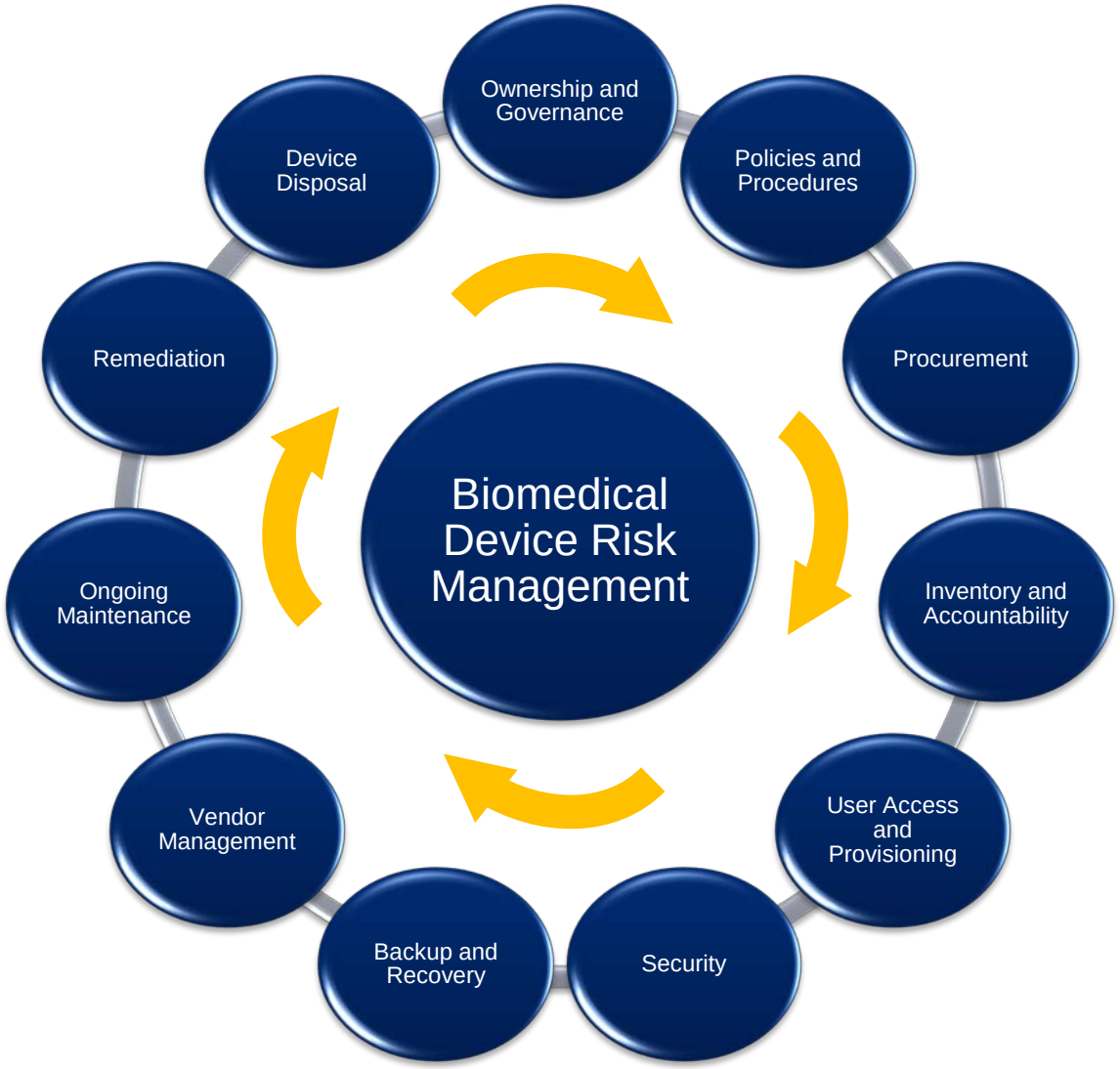
# Device Tracking

- Once you have an accurate inventory of devices, how are you going to keep this list updated?
  - Radio Frequency Identification (RFID)
  - Clinical Engineering Identification (CEID)
  - Service Set Identifiers (SSID)
  - Internet Protocol (IP) addresses
  - Media Access Control (MAC) addresses
  - Third party scanning tool
  - Manually
- Software solutions that can monitor devices on the network
- What information do you need to maintain about your devices?
  - Physical location, config changes, device activity, connectivity patterns
- Disposed or decommissioned devices – are they still discoverable and accessible?

# Challenges With Device Manufacturers

- Device manufacturers may not issue version updates
- Lack of regulation, and thus lack of enforcement
- FDA issues guidance, but not necessarily regulation
- The MDS2’s security controls for specific devices may not be publicly available
- Until patient safety has been negatively affected due to unsecure biomedical devices, significant change and enforcement may not occur.

# Biomedical Device Risk Management Lifecycle



# Polling Question #3

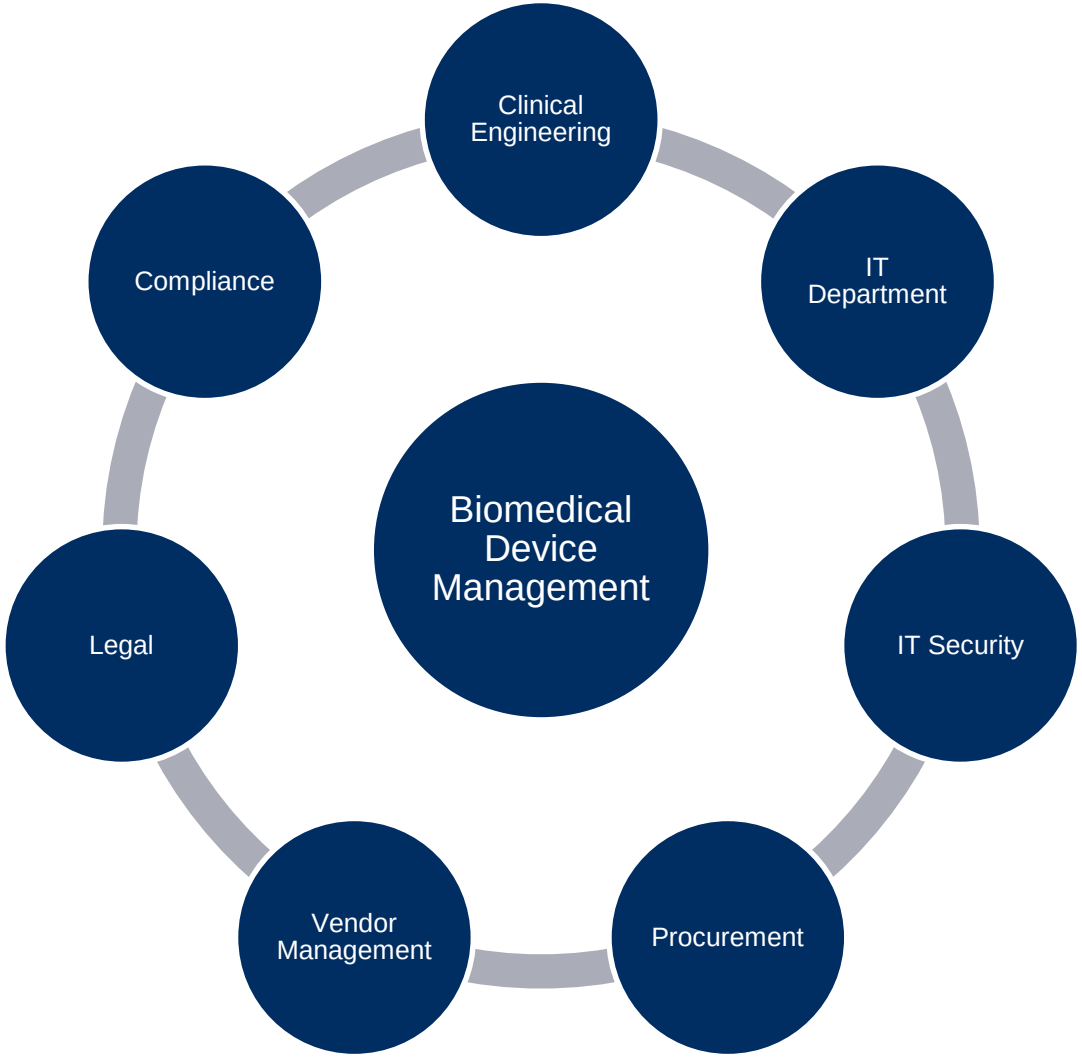
**What inventory method does your organization use to account for biomedical devices?**

a. RFID tagging
b. Standard asset tagging
c. Real-time network based identification
d. Periodic physical inventory
e. Rely on third-party to manage inventory
f. Unknown / Don’t know

# Governance - Who Should be Managing Biomedical Devices Within an Organization

# Biomedical Device Management Responsibilities - Governance

- Clinical Engineering
- IT
- IT Security (if outside of IT)
- Procurement
- Vendor Management
- Legal
- Compliance
- Others?
  - Facility leadership
  - Department heads
  - Data governance
  - Privacy
  - Finance



# Biomedical Device Management Responsibilities – Governance Challenges

- Typically isolated -  not enough representation or the appropriate representation
- Lack of committees providing governance
- Not visible to executive management
- No interest or engagement
- Simply not a priority in the organization and seen as a lower risk

# Polling Question #4

**What do you see your organization's greatest hurdle to provide effective biomedical device risk management? (check all that apply)**

a. Lack of good or comprehensive governance
b. Incomplete device inventory
c. De-centralized processes
d. Third-party risk management program gaps
e. Cannot secure the devices due to functionality or manufacturer proprietary limitations

# Takeaways / Summary

# Takeaways

- Communicate biomedical device risks; educate executive management, boards, leadership
- Select a cybersecurity framework and stick to it
- Understand what you can control
- Start with accounting for all medical devices – get assistance
- Implement a governance committee to oversee management of biomedical devices; get more stakeholders involved
- If you are in a governance, risk or compliance role, perform an assessment of biomedical device risk – get assistance where necessary

# Questions

# Thank you

**Robert L. Malarkey, CISSP, CISA**
VP, Healthcare Risk
Crowe Healthcare Risk Consulting
Office: +1 314 802 2040 | Mobile: +1 571 278 5438
robert.malarkey@crowehrc.com