MEDICAL DEVICE INTEROPERABILITY

THE IMPORTANCE OF CYBERSECURITY IN ASSESSMENTS

MD EXPO - 2025

NADIA ELKAISSI, BIOMEDICAL ENGINEER
JANE LACSON, BIOMEDICAL ENGINEER

INTRODUCTIONS

JANE LACSON

Biomedical Engineer,
Operations

NADIA ELKAISSI

Biomedical Engineer,
Medical Device Networking
& Cybersecurity

OVERVIEW

- IMPORTANCE OF CYBERSECURITY IN HEALTHCARE
- MEDICAL DEVICE INTEROPERABILITY
- CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY
- MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS
- CASE STUDIES
- BEST PRACTICES

IMPORTANCE OF CYBERSECURITY IN HEALTHCARE

MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

MEDICAL DEVICE INTEROPERABILITY

CASE STUDIES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

BEST PRACTICES

IMPORTANCE OF CYBERSECURITY IN MEDICAL DEVICES

10 - 15

Network-connected medical devices per patient bed

913,136

Total staffed beds in all US hospitals

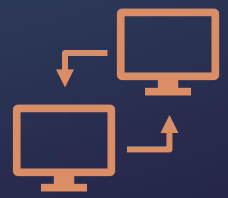
≈ 9.1 - 13.7 million

Network-connected medical devices in **all US hospitals**

RISKS POSED BY NETWORK-CONNECTED MEDICAL DEVICES

Increased bandwidth competition to the network

Increased risk for medical device exposure to malware



System integration challenges

Increased data storage requirements

Increased chance of loss of sensitive patient data stored on medical devices

CURRENT CYBERSECURITY THREATS

1. RANSOMWARE ATTACKS
2. AI - POWERED CYBER ATTACKS
3. SUPPLY CHAIN ATTACKS
4. IoMT VULNERABILITIES
5. CLOUD SECURITY THREATS
6. PHISHING AND SOCIAL ENGINEERING
7. QUANTUM COMPUTING THREATS
8. INSIDER THREATS

IMPORTANCE OF CYBERSECURITY IN HEALTHCARE

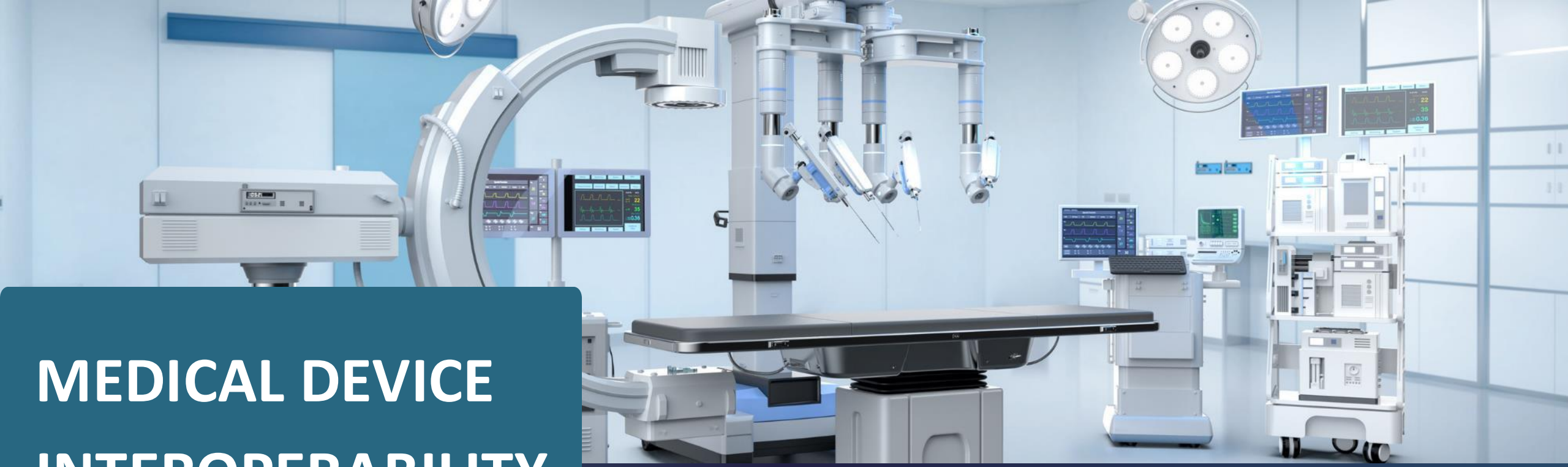
MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

MEDICAL DEVICE INTEROPERABILITY

CASE STUDIES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

BEST PRACTICES



MEDICAL DEVICE INTEROPERABILITY

The capability of medical devices to perform their intended functions safely, reliably, and consistently.

1

User Interface

Easy-to-understand controls for healthcare providers

2

Reliability

Minimizing the risk of malfunction during critical operations

3

Safety

Ensuring that the devices does not pose harm to patients or users

4

Integration

Ability to work with other medical systems for seamless patient care

IMPORTANCE OF CYBERSECURITY IN HEALTHCARE

MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

MEDICAL DEVICE INTEROPERABILITY

CASE STUDIES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

BEST PRACTICES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

01. Lack of Standardization

02. Usability and User Interfaces

03. Cybersecurity Threats

04. Integration with EHR

05. Compatibility Issues

06. Cost & Budget Constraints

CHALLENGES RELATED TO NETWORK CONNECTED MEDICAL DEVICES

CRITICAL FUNCTIONS

These devices often sustain life or provide vital clinical functions, making common security measures (e.g., inactivity timeouts) infeasible.

CUSTOM PLATFORMS

Although moving towards commercial OS platforms, many devices still use customized OS, specialized protocols, and closed architectures with unpublished specs.

OPERATIONAL CONSTRAINTS

Routine patching and applying agent-based protections (e.g., Host-Based Intrusion Prevention Systems - HIPS) can risk altering device functionality, impacting patient safety. Patching requires the original equipment manufacturer's consent.

TECHNICAL LIMITATIONS

Some devices lack the capacity for standard security controls (e.g., password logons).

Infusion Pumps: Often firmware-based

EKG Machines: Interfaces locked to medical diagnostic applications.

IMPORTANCE OF CYBERSECURITY IN HEALTHCARE

MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

MEDICAL DEVICE INTEROPERABILITY

CASE STUDIES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

BEST PRACTICES

MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments

IDENTIFY CONDITIONS

- **Where ePHI (electronic Protected Health Information could be:**
  - Used or disclosed without proper authorization
  - Improperly modified
  - Made unavailable when needed

UTILIZE RESULTS

- To make informed risk management decisions
- Implement security measures as required by the Security Rule

ACHIEVE RISK TOLERANCES

- Bring risk to ePHI within an organizationally established risk tolerance range
- Ensure a reasonable and appropriate level of security

DETERMINE ADDITIONAL CONTROLS

- Assess if additional security controls are necessary to protect ePHI

METHODOLOGY TO CONDUCT RISK ASSESSMENTS

1

IDENTIFY ASSETS TO BE PROTECTED

2

IDENTIFY DESIRED SYSTEM FUNCTIONS

3

IDENTIFY THREATS

4

IDENTIFY VULNERABILITIES

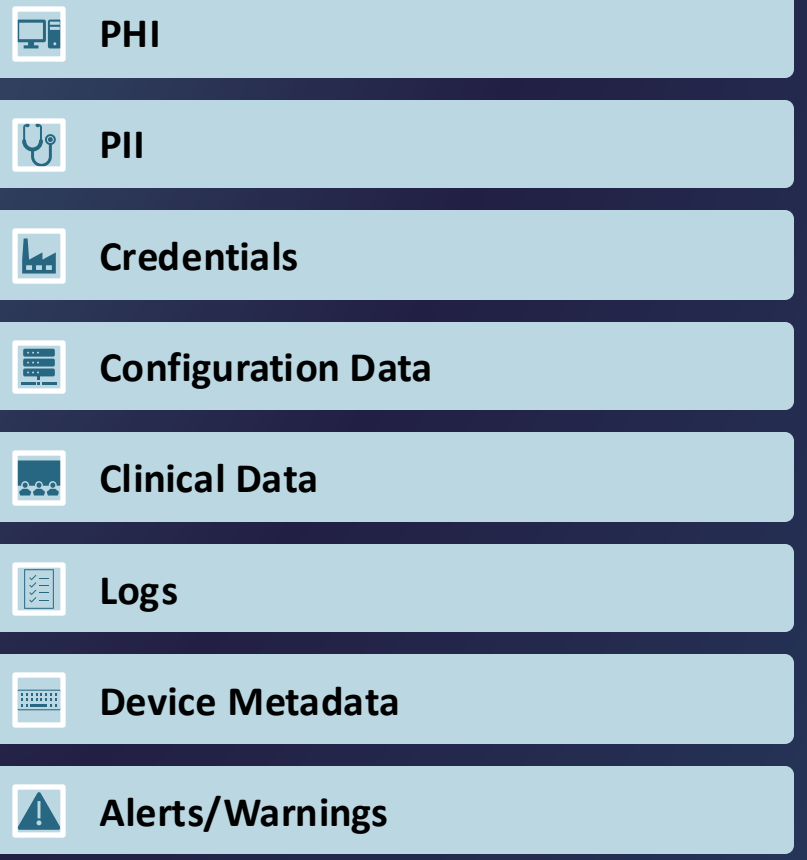
5

ANALYZE RISKS

6

IDENTIFY MITIGATION ACTIONS

IDENTIFY ASSETS TO BE PROTECTED



IDENTIFY DESIRED SYSTEM FUNCTIONS

- Device Setup and Configuration
- Inventory Tracking
- Identify devices in the network
- Deliver health-care services to patient
- Collect metadata on devices (logging, alerts, warnings)
- Secure data transmission
- Secure communications channel

IDENTIFY THREATS

- Malware
- Criminal Groups (e.g. black hat hackers, hacktivists, terrorists)
- Insiders
- National Governments
- Non-Human Events (e.g. utility outage, major disasters)
- Defective Equipment/Hardware
- Non-adversarial threats

IDENTIFY VULNERABILITIES

- Audit and Accountability Issues
- Wireless Communication Risks
- Outdated Technologies
- Patch Management Issues
- Authentication Weaknesses
- Security and Access Control Weaknesses
- Use of Removable Media
- Inadequate encryption protocols
- Inadequate physical protection of system

ANALYZE RISKS

Disruption of Operations

Information Disclosure/Loss/Theft

MITIGATION ACTIONS

- Implement Strong Access Controls
- Regularly Update & Patch Devices
- Encrypt Data
- Conduction Continuous Monitoring
- Employee Training and Awareness
- Develop and Test Incident Response Plans
- Segregate Networks
- Conduct Regular Security Audits
- Vendor Risk Management
- Implement Physical Security Measures

KEY COMPONENTS OF RISK ASSESSMENTS

- Ports, Protocols, and Services (PPS)
- MD/S Inventory
- Network topology diagram
- Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- Software Bill of Materials (SBOM)

ASK THE QUESTIONS

RISK ASSESSMENT KEY COMPONENTS - ASSET IDENTIFICATION

What is the device type? (Server, Discrete Device, Client)

Is it a standalone medical device or an integrated system?

Who manufactures the device?

What is the model of the device?

Who are the primary users of the device?

What is the primary function of the device?

List all systems needed for device functionality.

RISK ASSESSMENT KEY COMPONENTS - DEVICE SOFTWARE AND UPDATES

- What is the current software version of the device, and when is the next scheduled update expected to be released?
- Are software updates automated, or do they require manual intervention?
- What operating system does the device use?
- Can the operating system be automatically patched or what is the patching process?
- Does the device require support via an external connection? If so, are there processes in place to secure the connection?
- How does the manufacture address zero-day vulnerabilities?

RISK ASSESSMENT KEY COMPONENTS - DEVICE ACCESS/AUTHENTICATION

Does the device support the use of multi-factor authentication (MFA)?

Does the device require interactive login service accounts?

Does the vendor require a certain level of access to support?

How often are authentication credentials reviewed and updated?

If the device uses digital signature, is it compliant with FIPS 186-5?

MULTI-FACTOR AUTHENTICATION (MFA)

The United States Government is increasing MFA requirements

Executive Order 14028, Section 3(d)(i) and (d)(iii), which requires that agencies adopt MFA, report metrics on their adoption, and provide written justifications where unable to do so

The Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals (CPGs), Goal 2.H—Phishing-Resistant MFA, which recommends "add[ing] a critical, additional layer of security to protect assets accounts (sic) whose credentials have been compromised"

CHALLENGES FOR IMPLEMENTING MFA ON MEDICAL DEVICES

1. **Device Limitations:**
   - **Legacy Systems:** Many medical devices are built on older platforms without support for modern MFA methods.
   - **Hardware Constraints**: Limited processing power and memory may prevent the implementation of MFA.
2. **Usability Concerns:**
   - **Ease of Access:** In emergency situations, quick access is crucial. MFA might delay access to life-saving functions.
   - **User Burden:** Complex authentication processes can burden healthcare providers, affecting their workflow.
3. **Interoperability Issues:**
   - MFA solutions might not integrate well with existing medical device ecosystems or hospital IT infrastructure.

CHALLENGES FOR IMPLEMENTING MFA ON MEDICAL DEVICES

INCREASED RISK OF UNAUTHORIZED ACCESS	• Without MFA, devices are more vulnerable to unauthorized access, potentially compromising patient data and device functionality.
ALTERNATIVE SECURITY MEASURES	• Risk assessments must consider compensating controls such as physical security measures, network segmentation, and robust password policies.
COMPLIANCE RISKS	• Non-implementation of MFA may lead to non-compliance with certain regulatory standards, potentially resulting in penalties.
INCIDENT RESPONSE	• Enhanced monitoring, logging, and rapid incident response strategies become critical to mitigate potential security breaches.

PROPOSED SOLUTION: TAILORED METHOD FOR MFA

- **The underlying goal of mandated MFA is to address "low-hanging fruit" by removing the single-factor credential abuse threat vector**
- **Tailored methods can meet this same goal for medical devices**:

1. **Isolation and segmentation** of medical devices within the network
2. Implementation of **"indirect" MFA**
3. Implementation of **other access controls**, such as barcode scanning, Cisco ISE, etc.
4. External firewall monitoring for vendor remote access

RISK ASSESSMENT KEY COMPONENTS - DATA STORAGE/TRANSFER

- Does the device include a database? If yes, does the vendor support patching of the database?
- If there is a database, what is the database version and type?
- Does the device allow for encryption of the data drive or OS drives?
- What method of encryption is used for data in transit (SSL, HTTPS, TLS, etc.)?
- Is sensitive data stored at rest on the devices? If yes, how many records are stored and does the device support purging of data from local hard drive?
- Will sensitive be stored outside the hospital network (e.g. cloud-based environment)?
- Are backup and recovery systems in place for stored data?

RISK ASSESSMENT KEY COMPONENTS- NETWORK CONNECTIVITY

- What types of network connections does the device support? If wireless, does the vendor have a FIPS 140-2/3 certification #?
- What communication ports/protocols are NECESSARY for the system to be functional?
- What is the topology diagram of your system?
- How many IP addresses are necessary to network this device?
- Does the device utilize Bluetooth? If yes, which version? (Version 2.0, 2.1-4.0. 4. or newer)
- What type of vulnerability scanning is allowed on the device? Passive, Active, Both, Active-credentialed?
- Is external connectivity required for device operation?

UNDERSTANDING COMMUNICATION BETWEEN MEDICAL DEVICES AND EXTERNAL VENDORS/CLOUD-BASED SOLUTIONS

DATA SECURITY AND COMPLIANCE	•Ensures that both parties have a mutual understanding and agreement on the measures to protect sensitive patient data. •Helps to maintain compliance with relevant regulations and standards, such as HIPAA, GDPR, and NIST guidelines.
DEFINED ROLES AND RESPONSIBILITIES	•Clarifies the responsibilities of each party regarding data protection, system maintenance, and response to security incidents. •Establishes accountability, reducing confusion and enhancing coordination between the healthcare provider and the external vendor.
SECURE DATA TRANSMISSION	•Outlines the protocols and encryption methods used to protect data during transmission between the medical device and cloud-based solutions. •Minimizes the risk of data breaches and unauthorized access during data exchange.
INCIDENT RESPONSE PLANNING	•Specifies procedures for detecting, reporting, and resolving security incidents. •Ensures both parties are prepared to respond effectively to potential threats or breaches, minimizing impact on patient care.
PERFORMANCE AND RELIABILITY	•Sets expectations for system performance, uptime, and support, ensuring that medical devices function reliably and efficiently. •Details service level agreements (SLAs) to guarantee responsive support and maintenance from the vendor.

HIGH RISK PORTS

Port 23 (Telnet)	Telnet is an older protocol used for remote login sessions. It transmits data in plaintext, making it susceptible to eavesdropping and interception.
Port 21 (FTP)	The File Transfer Protocol (FTP) also transmits data in plaintext, which can be intercepted and manipulated. Secure alternatives like FTPS or SFTP should be used instead.
Port 445 (SMB/CIFS)	The Server Message Block (SMB) protocol is heavily used for file sharing. It has been exploited in numerous attacks, including the infamous WannaCry ransomware.
Port 3389 (RDP)	Remote Desktop Protocol (RDP) is popular for remote management but is often targeted for brute force attacks and exploits. It requires strong passwords and additional security measures.
Port 53 (DNS)	Domain Name System (DNS) services can be abused for DNS amplification attacks and other exploits. Monitoring and securing DNS queries and responses is crucial.
Port 80 (HTTP) and **Port 443 (HTTPS)**	These ports are used for web traffic. They need to be monitored for web application vulnerabilities such as SQL injection, cross-site scripting (XSS), and others.

HIGH RISK PORTS (CONT.)

Port 25 (SMTP)	The Simple Mail Transfer Protocol (SMTP) is commonly used for email transmission. It can be exploited for spam and phishing attacks if not properly secured.
Port 1433 (MSSQL)	The Microsoft SQL Server uses this port by default. Databases can be a goldmine for attackers, so monitoring and securing this port is essential.
Port 1521 (Oracle Database)	Used by Oracle databases, this port should be monitored to protect sensitive database contents from unauthorized access.
Port 3306 (MySQL)	Another database port, used by MySQL, which needs securing to prevent unauthorized data access.
Port 161 (SNMP)	The Simple Network Management Protocol (SNMP) is used for network management but can be exploited to gather information about network devices.
Port 69 (TFTP)	Trivial File Transfer Protocol (TFTP) is rarely used and lacks security features, making it vulnerable to attacks

CHALLENGES OF ACTIVE-CREDENTIALED SCANNING FOR MEDICAL DEVICES

Device Sensitivity

Regulatory Constraints

Proprietary Systems

Resource Limitations

CHALLENGES OF ACTIVE-CREDENTIALED SCANNING FOR MEDICAL DEVICES

IMPLICATIONS OF RISK ASSESSMENT

- Higher Risk Score
- Incomplete Security Profiles
- Reliance on Vendor Information

RISK ASSESSMENT KEY COMPONENTS - PHYSICAL SECURITY

Where is the device typically located within a facility (e.g., open area, secured room)?

What physical security measures are in place to protect the device in its typical location?

What types of authentication (e.g., PIN, biometrics) are required for gaining physical access to the device?

What measures are in place to ensure the durability and tamper-resistance of the device?

RISK ASSESSMENT KEY COMPONENTS - INCIDENT RESPONSE

Does the device have logging or other auditing mechanisms in place?

Does the device support backups?

Does the procurement include a backup solution? If so, what type?

How quickly can the device recover from an attack or malfunction?

Are there redundancies in place to maintain patient care during downtime?

IMPORTANCE OF CYBERSECURITY IN HEALTHCARE

MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

MEDICAL DEVICE INTEROPERABILITY

CASE STUDIES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

BEST PRACTICES

SCENARIO 1

A doctor recently procured an exciting new piece of equipment: a portable ultrasound device that can connect to a personal smartphone and store the imaging data in the vendor's cloud.

This cutting-edge technology offers enhanced mobility, allowing doctors to perform ultrasounds at the bedside or in remote locations, and review the results instantly on their phone. The data is stored in the cloud, making it easily accessible for further analysis and sharing with colleagues across multiple hospitals .

SCENARIO 1 - EVALUATION

DATA SECURITY	•The ultrasound stores imaging data in the cloud, which may pose risk related to data breaches, unauthorized access, or data leaks if not properly secured. Healthcare facilities need to ensure that the cloud storage complies with HIPAA and other data protection standards
NETWORK VULNERABILITIES	•The devices relies on a wireless connection to smartphones and cloud servers, which could be susceptible to network attacks.
AUTHENTICATION WEAKNESSES	•Inadequate authentication mechanisms can lead to unauthorized access to the device or the cloud storage.
PHYSICAL SECURITY RISKS	•As a portable device, the ultrasound is at a higher risk of loss or theft.

SCENARIO 2

A clinic adopted a new telemedicine platform to expand their remote consultation services amid increasing patient demand. The platform was integrated quickly, bypassing the standard risk assessment and cybersecurity review process. At the final stages, the system couldn't communicate with many of the systems in the hospital.

The vendor asks to remove all access controls and firewalls to allow for connectivity.

SCENARIO 2 - EVALUATION

INTEGRATION CHALLENGES	•Ineffective vetting of ports and protocols required for the platform led to extensive network configurations. The platform demanded over 30,000 ports to be opened, creating significant loopholes in network security.
NETWORK VULNERABILITIES	•The devices relies on a wireless connection to smartphones and cloud servers, which could be susceptible to network attacks.
AUTHENTICATION WEAKNESSES	•Inadequate authentication mechanisms can lead to unauthorized access to the device or the cloud storage.
PHYSICAL SECURITY RISKS	•As a portable device, the ultrasound is at a higher risk of loss or theft.

SCENARIO 3

Malware infects IT enabled network-connected medical devices through connection of infected removable media devices (for example, USB flash drive) used by vendors in maintenance activities or other device end users.

SCENARIO 3 - EVALUATION

OPERATION DISRUPTIONS	• Malware degrades performance of medical devices to a degree that they are unusable, or results in unreliable clinical data. Potential to infect other devices on same network.
NETWORK VULNERABILITIES	• If a device is not on a proper patch management policy, it is more susceptible to malware and viruses.
LOSS OF INFORMATION	• A compromised device may result in significant breach of sensitive data.
PHYSICAL SECURITY RISKS	• USB's are easily plugged into devices. Implementing physical locks on USB ports or disabled ports to mitigate. Have sign in's, training of staff, media scanning station.

SCENARIO 4 - EVALUATION

NON-ADVERSARIAL THREAT	• Lack of policies and procedures. MOU/ISA was not followed or not created. Using default passwords that accessed admin roles.
NETWORK VULNERABILITIES	• Remote login SOP was on public internet not behind any security page or login page. Full access to other documents in folder structure.
AUTHENTICATION WEAKNESSES	• Inadequate authentication mechanisms can lead to unauthorized access to the device or the cloud storage.
REMOTE ACCESS	• Can be exploited after discovering step by step instructions on gaining access

IMPORTANCE OF CYBERSECURITY IN HEALTHCARE

MEDICAL DEVICE CYBERSECURITY RISK ASSESSMENTS

MEDICAL DEVICE INTEROPERABILITY

CASE STUDIES

CHALLENGES IN MEDICAL DEVICE INTEROPERABILITY

BEST PRACTICES

BEST PRACTICES

The risk assessment process aims to uphold three key principles: safety, effectiveness, and data/system security.

Risk Management Framework

Create a risk management program that adheres to ISO 14971 and the NIST Cybersecurity Framework.

Keep a detailed inventory of all connected medical devices.

Vulnerability Assessment

Perform regular scans and tests to detect threats such as malware and unauthorized access.

Assess the consequences of breaches on patient safety and the integrity of data.

Security Controls and Training

Put measures in place such as encryption and access controls.

Ensure that devices are regularly updated.

Provide training for staff on cybersecurity practices and how to respond to incidents.

Monitoring and Vendor Management

Keep an eye on devices for any unusual activity and establish a response plan.

Collaborate with manufacturers to ensure that security measures are incorporated from the design phase all the way through to deployment.

CONCLUSION

- Improve decision-making during the evaluation and acquisition of new medical devices
- Enhanced safety, reliability, and security in medical technology
- Working and integrating evolving security initiatives to improve Data/System Security but not compromising the safety and effectiveness of the device.

THANK YOU

FOR YOUR ATTENTION

MD EXPO - 2023