HONORHEALTH®

Medical Device Cybersecurity Fundamentals

Presented by:
Lynn Holland & Jessica Pitterka

About Your Presenters

HONORHEALTH®

Jessica Pitterka, MSCIA

Clinical Asset Defense Engineer at HonorHealth

Jessica is a healthcare cybersecurity leader specializing in medical device security, risk governance, and the protection of complex clinical environments. She holds a Master of Science in Cybersecurity and Information Assurance and brings deep expertise in designing and operationalizing security programs that safeguard connected medical technologies without compromising patient care delivery.

Lynn Holland

Director of HTM at HonorHealth

Lynn is a healthcare technology leader with a unique clinical and operational background, built on prior service as a U.S. Air Force flight nurse and 24 years with HonorHealth holding progressive leadership roles across IT, Supply Chain, and Healthcare Technology Management, bringing a cross-functional perspective to improving operational efficiency, technology integration, and patient care delivery.

Intro to Medical Device Security

HONORHEALTH®

What is Medical Device Security?

- Practices, processes and technologies to protect medical devices from cyber threats
- Managing risk
- Reduce likelihood and impact of a cyber incident
- Balancing clinical usability with safety
- Spans many pillars – vulnerability management, change management, network segmentation

Why it Matters

- Direct impact on patient safety and operations
- Connected devices are everywhere
- Increased cyber threats targeting hospitals

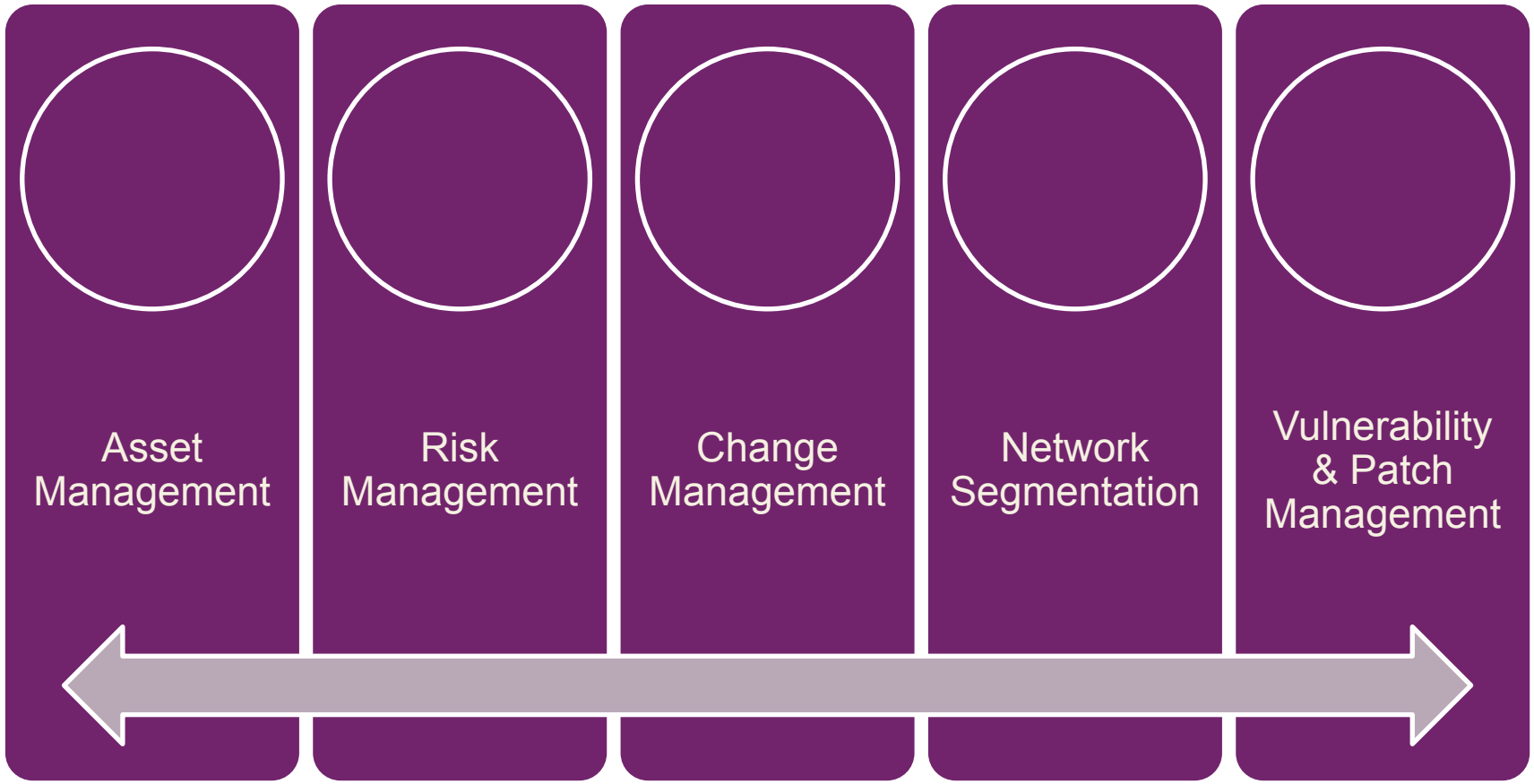
The Challenge

- Balancing clinical need and security
  - Accessibility vs confidentiality
- Communication gap
- Legacy systems
  - High replacement cost
  - Difficult to secure
- Vendor controlled devices – Vendor HW
- Vendor resistance (citing FDA)
- Limited patching ability
- Integrations

The Pillars

HONORHEALTH®

Program Fundamentals Overview



Implementation Roadmap

Start simple. Build momentum. Mature over time.

Phased approach

- 4. Optimize
- 3. Operationalize
- 2. Risk Reduction
- 1. Visibility

Pillar	1. Visibility	2. Risk Reduction	3. Operationalize	4. Optimize
Asset Management	▯ Models & assets are managed ▯ Asset attribute tracking ▯ Models containing PHI are identified. ▯ Deploy IoT Solution	▯ Track MDS2 & Risk summary in CMMS ▯ Track core hardware components ▯ New equipment on network is monitored	▯ Models & assets are standardized ▯ IoT solution and CMMS are integrated ▯ Asset decommissioning process	▯ Integrate IoT with NAC, SIEM, FW, and vendor portals ▯ Asset lifecycle management
Risk Management	▯ Complete risk assessments for medical devices	▯ Prioritize corrective action plans	▯ Remediate risk	▯ Vendor risk management
Change Management	▯ Define change management process	▯ Evaluate high impact changes	▯ Implement change management	▯ Expand & mature change management
Network Segmentation	▯ Evaluate current medical device segmentation	▯ Evaluate high risk medical devices ▯ Profile devices	▯ Segment medical devices	▯ Automate segmentation
Vulnerability & Patch Management	▯ Track vulnerabilities	▯ Evaluate vulnerability risk & prioritize	▯ Remediate vulnerabilities	▯ Automated risk evaluation & prioritization

Asset Management

HONORHEALTH®

Asset Management Details

Connecting CMMS with IoT

- Automate data exchange to eliminate manual errors
  - check and balance for population of MAC Address, IP Address, version of software, etc.
- Improve inventory accuracy and completeness
- Identify missing, underused, or unregistered devices
  - measure offline devices for utilization and PHI management
- Create a single source of truth for asset management within the CMMS
- Added benefit: Link CMMS with IoT and AP Mapping for real-time asset tracking

Pillar 1 - Asset Management

Main Goal: Inventory Visibility -
Establish a complete and continuously updated inventory of all medical devices on the network.

How to Achieve It:

Path 1: Automated Data Collection

1. Deploy passive network discovery tools / IoT Solution
2. Bi-directional integration between CMMS/CMDB inventory and IoT Solution
3. Continuously validate discovered devices against known inventory

Path 2: Manual Data Collection

1. Hire additional Biomedical Technicians or an Inventory Management Specialists
2. Physically round to locate every piece of equipment & collect required information
3. Enter data into CMMS
4. Continuously monitor (newly acquired) equipment

Vulnerability & Patch Management

HONORHEALTH®

Pillar 2 – Vulnerability & Patch Management

Main Goal:
Reduce exposure to known vulnerabilities while maintaining clinical uptime.

How to Achieve It:

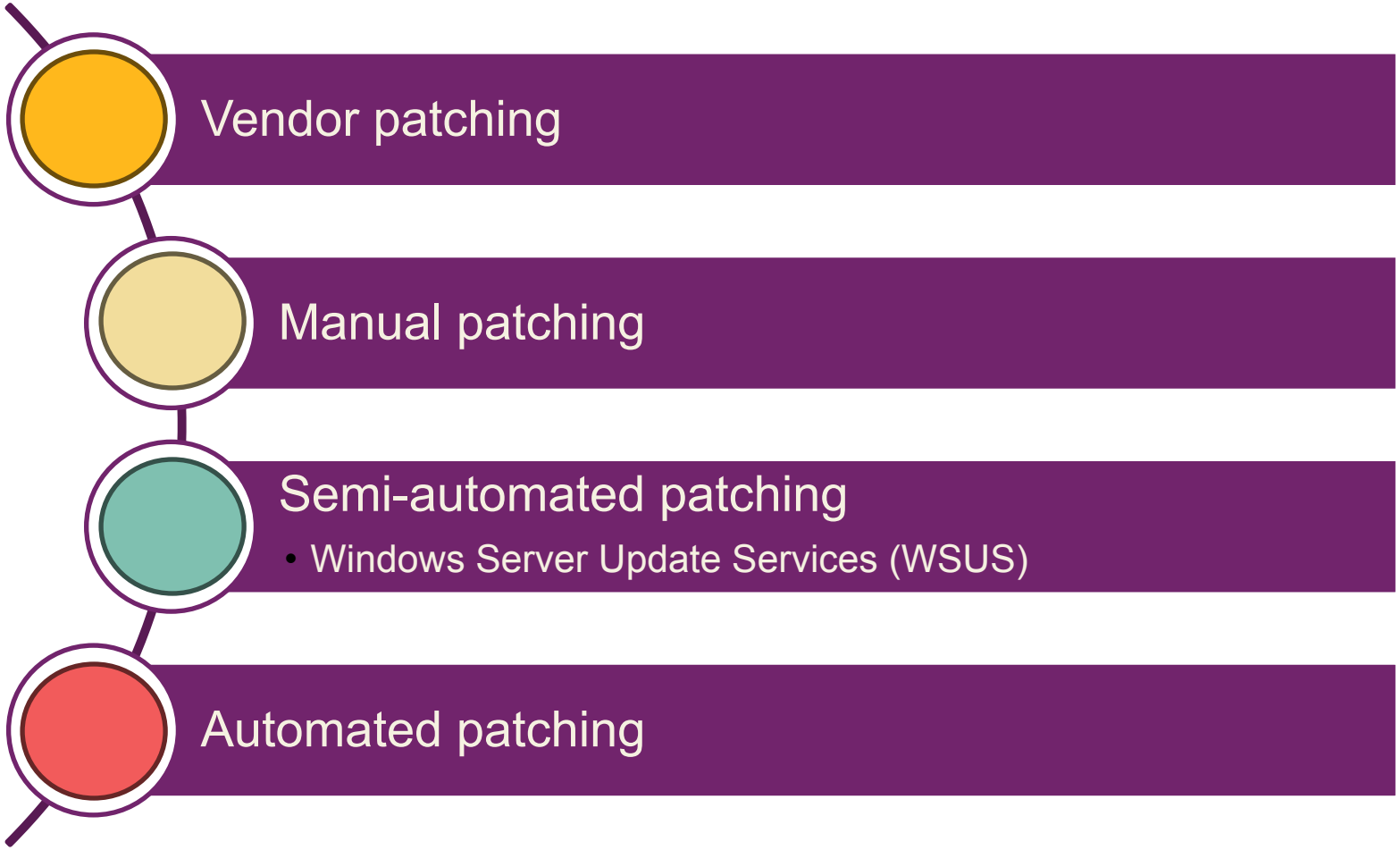
Path 1: IoT Automated Vulnerability Management

1. IoT solution automatically tracks vulnerability status across all connected medical devices
2. Prioritize remediation based on risk scoring and exploitability
3. Coordinate remediation with vendor
4. Patch devices or apply compensating controls

Path 2: Manual Tracking & Prioritization

1. Find and track disclosed vulnerabilities from various sources
2. Perform vulnerability scans in controlled environments
3. Track CVEs relevant to device inventory
4. Manually evaluate risk scoring and remediation priority
5. Coordinate remediation with vendor

Patch Management



Risk Management

HONORHEALTH®

Pillar 3 – Risk Management

Main Goal: Risk Identification, Classification & Prioritization
Identify & prioritize security efforts based on clinical and operational risk.

How to Achieve It:

Path 1: IoT Enabled Automated Risk Classification

1. IoT solution identifies and classifies risk
2. Automatically assigns risk scores using behavioral analytics
3. Update risk rating based on network activity, vulnerabilities and device behavior
4. Feed results into CMMS/CMDB and/or SIEM for real time visibility
5. Manage & remediate risk

Path 2: Traditional Risk Scoring Model

1. Define risk scoring model
2. Categorize devices into risk tiers
3. Evaluate devices against risk scoring model
4. Manually track risk
5. Create remediation plan
6. Manage & remediate risk

Traditional Risk Scoring

Likelihood	Minimal 1	Minor 2	Moderate 3	Significant 4	Severe 5
Almost Certain 5	Medium – 5	High – 10	Very High – 15	Extreme – 20	Extreme – 25
Likely 4	Medium – 4	Medium – 8	High – 12	Very High – 16	Extreme – 20
Possible 3	Low – 3	Medium – 6	Medium – 9	High – 12	Very High – 15
Unlikely 2	Very Low – 2	Low – 4	Medium – 6	Medium – 8	High – 10
Very Unlikely 1	Very Low – 1	Very Low – 2	Low – 3	Medium – 4	Medium – 5

Impact

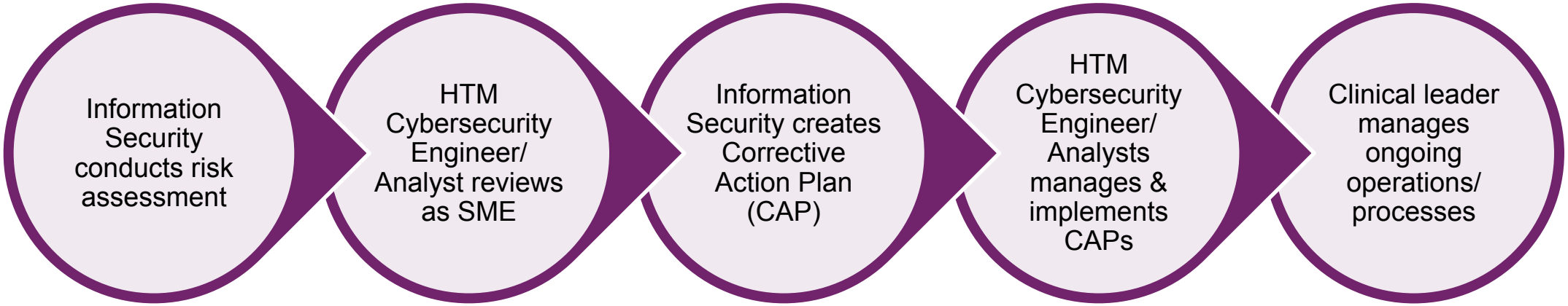
Scenario – a patient monitoring device is running an outdated software with a known vulnerability that could allow unauthorized network access.

Step 1: Assign Likelihood score
Step 2: Assign Impact score
Step 3: Calculate Risk score

Formula: Likelihood x Impact

Risk Assessments for New Medical Devices (Pre-Deployment)

Main Goal:
Evaluate cybersecurity risk before a device is introduced into the clinical environment.



Key Inputs:

1. MDS2 (Manufacturer Disclosure Statement for Medical Device Security)
2. Vendor security architecture documentation
3. Clinical use case
4. Network placement (clinical team & networking) & Network diagram (vendor)

Network Segmentation

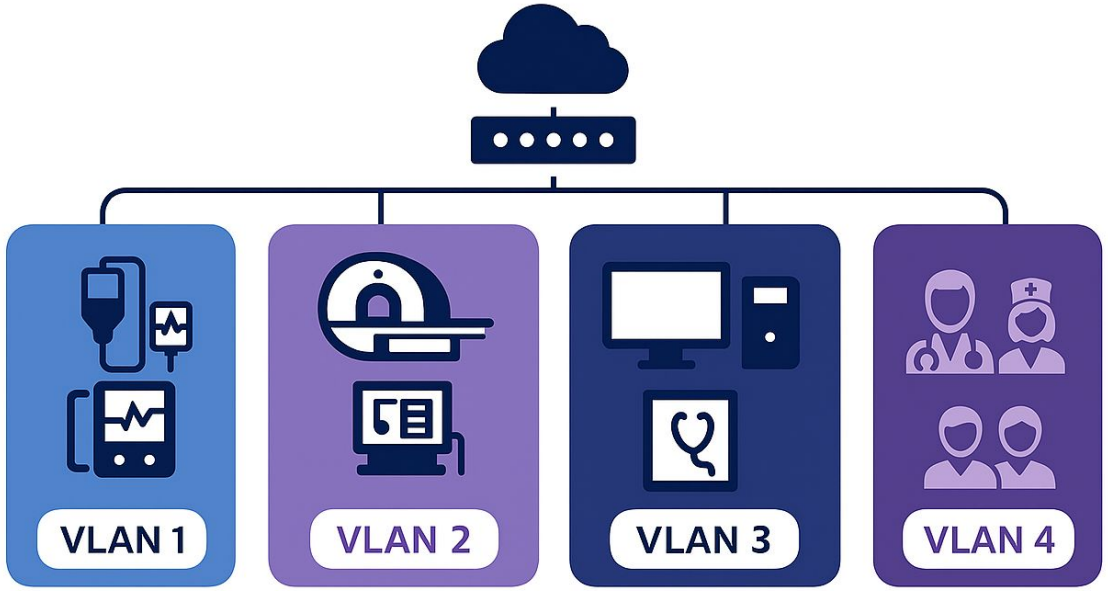
HONORHEALTH®

Pillar 4 – Network Segmentation

Main Goal:
Reduce attack surface and prevent lateral movement between devices and enterprise systems.

How to Achieve It:

1. Implement VLANs / microsegmentation (Zero Trust)
2. Separate clinical devices from corporate network
3. Restrict east-west traffic, allow only necessary ports & protocols



P4. Network Segmentation

Path 1: Traditional VLAN Segmentation

How to Achieve It:

1. Identify devices
2. Work with networking to create VLANs and Firewall rules
3. Re-IP the devices (as needed)

Cons:
- Increased ongoing maintenance
- Vendor cost for IP change

VLAN Example	Category	Example Devices
200	Bedside monitoring	Vital Signs Monitors, Patient Monitors
210	Infusion & Therapy	Infusion Pumps
220	Life-Critical Real-Time Devices	Ventilators, Anesthesia
230	Imaging Modalities	CT, MRI, Ultrasound, X-Ray
240	Cardiology & Diagnostic Systems	Cath Lab, Hemodynamics, ECG
250	Laboratory Devices	Blood Analyzers, Hematology Analyzers, Pathology Instruments
260	Surgical Systems	Surgical Navigation, Robots & Consoles
270	Legacy Imaging Devices	Windows XP, Windows 7 - Imaging
280	Legacy Diagnostic Devices	Windows XP, Windows 7 - Diagnostic
290	Legacy Laboratory Devices	Windows XP, Windows 7 - Lab
300	General Biomedical Equipment	Any Other

P4. Network Segmentation

Path 2: Identity Based Segmentation – Zero Trust

How to Achieve It:

1. Evaluate identity (Active Directory, certs), device type (profiling)
2. Assign tags based on information
3. Define group rules
4. Implement group rules

Change Management

HONORHEALTH®

Pillar 5 – Change Management

Main Goal: Implement a controlled, auditable process for all changes impacting medical devices.

How to Achieve It:

1. Establish or tie into existing change control process (Change Advisory Board or equivalent)
2. Require operational impact risk assessment before implementing changes
3. Peer review change prior to deployment and approval
4. Schedule changes during approved maintenance windows
5. Document and track all changes for auditability

P5. Change Management

What needs to go through change management?
- Patches
- Upgrades
- Configuration changes
- Network changes

What needs to be evaluated?
- Patient safety impact
- Downtime & clinical workflow disruption

Who needs to be involved?
- Clinical Engineering / HTM
- IT
- Information Security
- Clinical Leader

What needs to be considered?
- Test environment if possible
- Device validation
- Network behavior
- Security controls

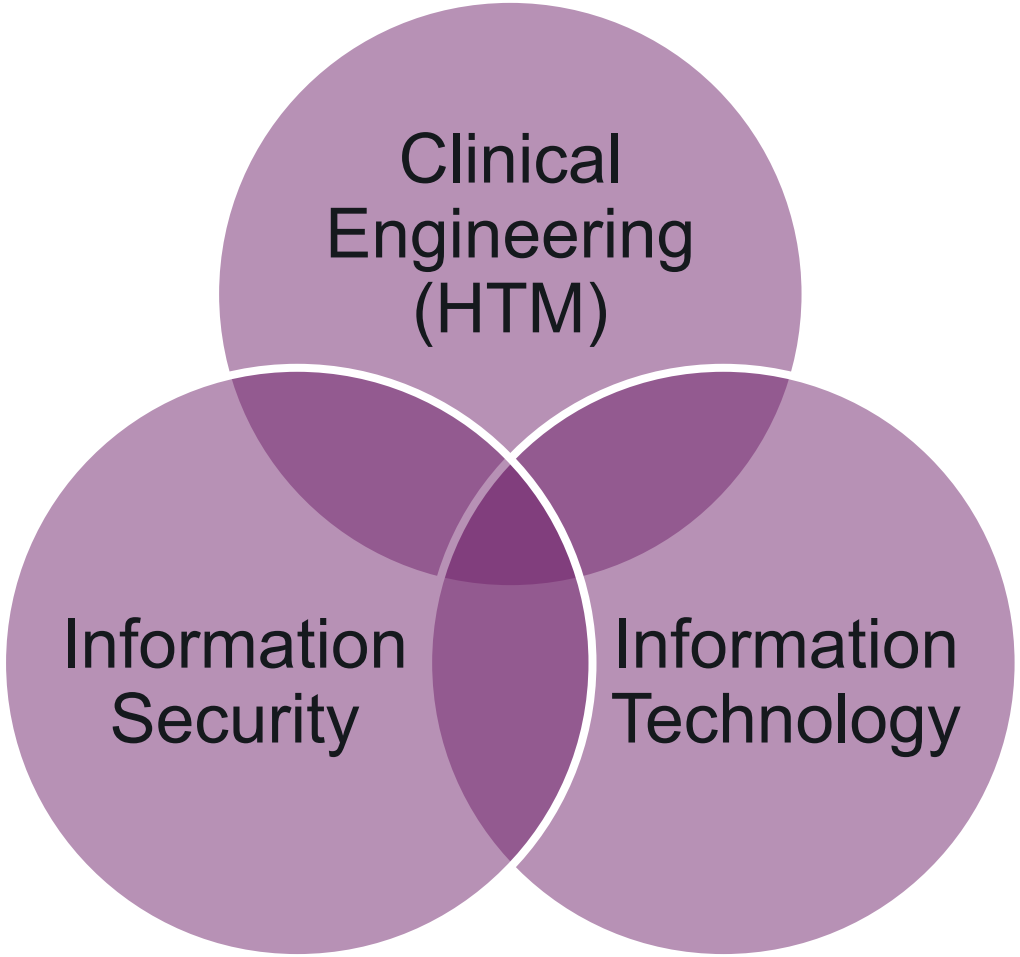
How do I implement a controlled change?
- Schedule change to minimize clinical impact
- Use maintenance windows when applicable
- Ensure rollback plans are defined

What do I need to document?
- Any updates to the asset
- Configuration baseline changes
- Network diagrams
- Integration

Governance

HONORHEALTH®

Ownership



Collaboration is Essential

Policy & Vendor Management

- Define cybersecurity policies that establish acceptable risk levels, lifecycle governance, and security requirements for medical devices
- Embed cybersecurity language into contracts (MSAs, BAAs, SLAs) to hold vendors accountable for patching, vulnerability disclosure, and incident response
- Set clear procurement requirements to ensure devices meet security standards before purchase (e.g., FDA, NIST, SBOM transparency)
- Engage vendors early in the device lifecycle to align on security expectations from selection through deployment
- Conduct vendor risk assessments and ongoing performance monitoring to ensure continued compliance
- Recognize cybersecurity as a continuous process, not a one-time activity, requiring ongoing maintenance, review, and updates to address evolving threats

What Good Looks Like

Risk Based Approach

Strong Collaboration

Continuous Visibility & Improvement

Q&A