Medical Device Patch Management
Factors for Strategy and Execution

Ron Mehring, Vice President – Technology & Security, Texas Health Resources
Axel Wirth, Distinguished Technical Architect, Symantec Corporation

March 1st, 2016

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.
Conflict of Interest

Ron Mehring, MBA, CISSP
Has no real or apparent conflicts of interest to report.

Axel Wirth, CPHIMS, CISSP, HCISPP
Has no real or apparent conflicts of interest to report.

Presentation developed with support from Andrew Sargent (Philips) and Dr. Dale Nordenberg (MDISS)
Agenda

• Medical Device Security Introduction
• Regulatory Landscape
• Manufacturer Requirements under FDA Quality Rule:
  – Challenges of Complexity
  – Patch Management – Challenges for Medical Device Manufacturer
  – FDA Quality Rule
  – Manufacturer Best Practices
• Patch Management – Challenges for Healthcare Delivery Organizations
• Patch Management Process
  – Device IT Security Profile
  – Asset Risk Profiling
  – Patch Management Process Examples
• Tactical measures to limit risk exposure
  – Limiting Risk
  – Compensating Controls
• Wrap-up and Summary
• Discussion
Learning Objectives

1. Explain the regulatory, policy, and operational challenges of medical device patching

2. Illustrate the primary components of a comprehensive medical device patch management program

3. Outline the limitations of medical device patching and propose mitigating controls
Benefits Realized through a Mature Patch Program

**Satisfaction:**
- Avoid downtime and patient / staff frustration

**Treatment / Clinical:**
- Maintain clinical operations
- Improve patient safety

**Electronic Secure Data:**
- Enable medical device integration while maintaining security and compliance

**Patient Engagement and Population Management:**
- Maintain patient trust

**Savings:**
- Avoid costly downtime, fines, and impact on reputation
Medical Device Security is an emerging discipline and area of focus for Medical Device Manufactures and Health Care Delivery Organizations (HDO’s).

- There has been much industry confusion about the regulatory landscape surrounding medical device security, and patching in particular.
- The FDA has repeatedly provided clarification through multiple written guidance documents and communications, yet confusion remains.

**We hope to use this presentation time to add to the collective wisdom of the industry in order to evolve the conversation and provide valuable strategic insights to the audience.**

- It is important to remember that patch management is only one cornerstone to secure systems, networks and environments.
- Hospitals must provide appropriate risk assessment and mitigation via security controls in order to reduce exposure.
- The industry at large is still evolving in their understanding and handling of medical device cybersecurity.

In order to be successful, hospitals, healthcare environments, manufactures and FDA regulators need to work together to collectively evolve in order to deliver the most secure systems possible.
The World we Live in

A changing Cyberthreat Landscape:
- Unprecedented numbers of new malware (millions/day)
- Increasingly targeted and sophisticated attacks
- Social engineering, “under the radar” attacks
- Changing attack motivation:
  fame → fortune → organized crime → cyber-warfare / -terrorism
- Everybody is at risk – nations attacking companies; hacktivism & social causes
- Separation of motivation and capability - hackers for hire, underground economy

A changing Healthcare Ecosystem:
- Market drivers: cost pressure, need to improve efficiency, aging population
- Government stimulated digitization (HITECH)
- Increasing integration of devices and backend systems (EHR, PACS)
- New care delivery models (home care, mHealth, health-IoT)
- Patient and provider mobility (BYOD, anytime anywhere access)
Introduction to Medical Device Security

Why is it such a focus now, as compared to a few years back?

Main Events:

2008 – Pacemaker hack (Kevin Fu, UMass Amherst).

2011 – Insulin Pump hack (Jerome Radcliffe, Black Hat Conference).


2014 – FBI Alerts to Healthcare Industry, NIST NCCoE Medical Device Use Case project launched, AAMI/ECRI safety warning on cybersecurity risks.


2015 – HHS OIG announced that it will include networked medical devices in upcoming audits.

Introduction to Medical Device Security

Do we know how bad it is? Examples of Incidents:

Anecdotal:
– Med Cabinet and Cathlab shutdown (Malware introduced via USB)
– Ultrasound Systems sending spam email (Botnet)
– Manufacturer introduced: malware on new devices; download site infected; malware in on-device PDF manual.

Published:
– Patient drug abuse (infusion pump safety override, published password)
– Device theft (PHI breach)
– TrapX (May 2015): Medical Device Hijack (device as attack beachhead)
– Protiviti (Sept. 2015):
  • MRI and Defibrillator “honeypots”: 55,416 login attempts, 299 attempts to install malware, and 24 exploits of Conficker vulnerability detected over 6 months.
  • Also found 68,000 Internet-exposed Medical Devices from one health group.

Security Testing & Research:
– DHS (2013): 300 devices, 40 vendors – security issues (e.g. hard coded PW)
Complexity is part of the problem. It is a true “System of Systems” challenge – on all levels: technical, organizational, operational, and impact potential. This complexity creates challenges when implementing a traditional asset and risk management approach for the medical device ecosystem.
How to Approach Cybersecurity

**Device:**
- Hardening
- On-device Security
- Privacy & Data Protection
- Password Management
- Secure (remote) Access
- Maintenance & Patching
- Vulnerability Disclosure

**Network:**
- Segregation (VLAN)
- Network Security Monitoring
- Access and Traffic Control

**Process:**
- Procurement
- Vulnerability Analysis
- Security Education
- Use and Handling
- Lifecycle & Change Mgmt. (incl. patching)
- Asset & Risk Mgmt.

Patching is an essential part of maintaining device’s security posture.

**What it does:**
- Keeps OTS (commercial & open source) up to date
- Protects against recently discovered vulnerabilities
- Complements other security measures (hardening, anti-malware, whitelisting)

**What it does not do:**
- Protect against zero-day vulnerabilities
- Protect against all attack vectors (e.g. password theft)
- Eliminate the need for other security measures (e.g. network)
Cybersecurity – how to approach it

But - Patching can be challenging:
• Timely release by Manufacturer
• Timely deployment by HDO
• Change management
• Device dependencies (all or none)
• Dependency on other backend systems (workstations, servers)
• Responsibility & communication

Commercial off-the-shelf (COTS) and Open Source Software are the primary concern:
• Operating System
• Network Stack
• Runtime Environment (Java)
• Readers, Media Players, Browsers
• Databases
• … any other commercial software

Patching should be part of:
• Manufacturer Quality System Processes
• HDO Lifecycle Management
• HDO Asset Management (know all components & configuration)
• HDO Risk Management (risk changes with configuration)
• Manufacturer to HDO communication (and contract)
Regulatory Complexity – Overlaps and Gaps

- FDA: Safety and Effectiveness
- HHS: Assure C-I-A of ePHI (HIPAA)
- The Joint Commission: Medical Equipment Safety (EC 02.04.01)

Medical Device Cybersecurity: Regulatory Overlap yet Execution Gaps

Other Stakeholders:
- FBI – Crime Prevention
- DHS – National Security
- FTC – Consumer Protection
- FCC – Wireless Reliability
- NIST – Standardization (national)
- ISO – Standardization (global)
- UL – Assurance & Certification
- IEEE – Engineering Frameworks
- Others: HIMSS, AAMI, IHE, VA/DoD, MDISS, Mitre, NEMA, …
US Food and Drug Administration (FDA)

Evolving view on Off-the-Shelf (OTS) software

“Guidance for Industry on Compliance of Off-the-Shelf Software Use in Medical Devices”

“Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”

“Content of Premarket Submissions for Mgmt. of Cybersecurity in Medical Devices - Guidance for Industry”

Draft: Postmarket Management of Cybersecurity in Medical Devices

1999

• Treating OTS software like any other device component:
  • Requires documentation
  • Include in verification & validation
  • Specific hazard analysis and mitigation
  • Describe residual risk

2005 (2009)

• Cybersecurity requires software lifecycle mgmt. = patching
• Clarified that:
  • Vulnerabilities can affect safety
  • Cybersecurity is part of the manufacturer’s Quality System and Corrective Action Plan
  • Security patches do not require resubmission to the FDA

2014

• Manufacturer responsibility:
  • Limit unauthorized access
  • Ensure trusted content
  • Provide a fail-safe mode
  • Retention & recovery
• Documentation:
  • Hazard analysis, mitigation
  • Cybersecurity controls
  • Patching & lifecycle mgmt.
  • Security instructions

2016

• “Essential Clinical Performance”
• ISAO
• Inf. Sharing Analysis Org.
• Certain protections
• Clarification on Security Patches and Updates
• Vulnerability mgmt.

SW as a static component

SW’s unique lifecycle mgmt. & security needs

Software system cybersecurity needs

Transparency & vulnerability sharing
Manufacturer Requirements under FDA Quality Rule:

• Under FDA Title 21 CFR 820 'Quality Rule', manufacturers are required to perform a Safety Risk Assessment and Hazard Analysis (ISO 14971).
• Security updates that do not impact device functionality or intended use do not require manufacturer FDA filing or approval (i.e. 510(k) or PMA).
• BUT – security updates still need to be managed under the manufacturer's Quality System (hazard analysis, formal testing and release)

Beyond the FDA - other Regulatory Considerations:

• Approval requirements in other international regions may vary.
• Although manufactures are not regulated by the HIPAA Security Rule, they need to enable their customers to comply - protect C-I-A of ePHI.
FDA Guidance (Oct. 2014):

- **Identify & Protect**
  - Limit access to trusted users
  - E.g. no common or hardcoded passwords
  - Ensure trusted content

- **Detect, Recover, Respond**
  - Detect, recognize, log, and act upon security incidents
  - Actions to be taken
  - Protect critical functionality
  - Recover device configuration

- **Cybersecurity documentation**
  - Hazard analysis, mitigation, design considerations
  - Traceability matrix (cybersecurity controls to risks)
  - Update and patch management
  - Manufacturing integrity
  - Recommended security controls

FDA Postmarket Guidance (Draft Jan. 2016):
- Cybersecurity is a shared responsibility
- “Information Sharing Analysis Organization”
  - ISAO - Multi-Stakeholder
  - Voluntary but: actionable, transparent, trusted
  - Information shielded from release, exempt from regulatory use and civil litigation
  - Critical component of a comprehensive approach to cybersecurity
- Introduces “Essential Clinical Performance”
- “Cybersecurity routine patches and updates”
  - Generally not required to be reported
  - Unless serious adverse health consequences or unacceptable residual risk
- Other key Manufacturer guidance:
  - Threat and incident monitoring
  - Vulnerability disclosure policy
  - Receive and process vulnerability reports
  - Practice good cyber hygiene
Manufacturer Requirements under Jan 2016 Draft Guidance:

- Introduces several new concepts:
  - “Essential clinical performance” – freedom from unacceptable clinical risk
  - “Controlled” vs. “uncontrolled risk” - acceptable vs. unacceptable residual risk
  - “Routine updates and patches” – increase security, reduce vulnerability, but not routine if intended to reduce risk to health or correct a violation

<table>
<thead>
<tr>
<th></th>
<th>Controlled Risk</th>
<th>Uncontrolled Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential Clinical Performance</td>
<td>Sufficiently low (acceptable) residual risk</td>
<td>Compromised; unacceptable risk</td>
</tr>
<tr>
<td>Manufacturer Action</td>
<td>Good cyber hygiene and risk reduction are encouraged</td>
<td>Remediate; advise on temporary risk mitigation</td>
</tr>
<tr>
<td>Reporting to FDA</td>
<td>Generally not required when providing “routine update and patches”</td>
<td>Mandatory, except:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- No known serious events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Bring risk to an acceptable level within 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Mfr participating in an ISAO</td>
</tr>
<tr>
<td>Class III/PMA devices</td>
<td>Include in periodic (annual) reporting</td>
<td>Include in periodic (annual) reporting</td>
</tr>
</tbody>
</table>

Note – this slide is a highly summarized interpretation of the FDA guidance, please refer to the actual document for regulatory and legal advise.
Manufacturer Best Practices:

• Address cybersecurity during design and development of the medical device, resulting in more robust and efficient mitigation of patient risks.

• Manufacturers should establish a cybersecurity vulnerability and patch management approach as part of the software validation and risk analysis.

• The expectation is that cybersecurity updates to software are:
  • Required to maintain a product’s safety and effectiveness
  • Patch approval is the responsibility of the manufacturer
  • Patch deployment is a shared responsibility of manufacturer and HDO

• We have to assume that a device will be operated in a “hostile cyber-environment” (i.e. the hospital network) and responsible vulnerability management is part of devices’ lifecycle management.

• Traditionally, focus was on “intended use and reasonably anticipated misuse”. With regards to cybersecurity, this is now evolving to include “malicious and intentional misuse”.

• Provide Vulnerability Disclosure Policy and enable Vulnerability Reporting.
  • Document device security posture, new vulnerabilities, security recommendations and compensating controls.
Manufacturer Best Practices

Example best practices for manufactures to support a well defined patch and vulnerability management program

Typically, medical device manufacturers should:

- Continually monitor threats and vulnerabilities
- Have a vulnerability disclosure policy in place.
- Provide clear and timely communication on known (including newly discovered) vulnerabilities and mitigation (e.g. patch).
- Have a defined lifecycle policy, including an SLA on patch and upgrade availability.
- Patches for OS, Middleware and Application may be bundled or released separately, depending on use-case

**Design with security best practices:**
Minimize security risks and lifecycle management pressures through:

- OS Hardening,
- Minimize attack surface (install only required components, close unused ports, etc.)
- Utilize complementary security technologies (e.g. whitelisting, firewalls).
- Refrain from bad design practices, e.g. simple, hard-coded, or default passwords
**Manufacturer Challenges**

Medical Device Manufactures must meet mandated regulatory requirements, customer demands and support proper safety and security assessments in accordance with the Quality System Rule

<table>
<thead>
<tr>
<th>Primary regulatory duty is Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FDA Quality System Rule (Title 21-Section 820)</td>
</tr>
<tr>
<td>• Issues resulting from safety focus (ISO 14971) and “intended use” concept</td>
</tr>
<tr>
<td>• Manufacturers are not regulated by HIPAA (although their customers are)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Costly Assessments for Post-Sale Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Time and resources to perform engineering analysis, verification &amp; validation, formal release &amp; customer notification</td>
</tr>
<tr>
<td>• Validation required for multiple product portfolios and device versions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specifically, full OS Upgrade Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Full OS upgrade may not be technically or economically feasible</td>
</tr>
<tr>
<td>• May also drive costly hardware upgrade.</td>
</tr>
<tr>
<td>• May require regulatory filing in some countries</td>
</tr>
<tr>
<td>• But - may be able to extend life with supplementary security measures (e.g. whitelisting)</td>
</tr>
</tbody>
</table>

**Other manufacturer challenges:**

• Long product life
• Customer education
• Differences in customer requirements and expectations

In general, these constraints make it difficult to be nimble with security design changes and updates
Health Care Delivery Organization Patch Management Challenges

Health Care Delivery Organizations face multiple challenges around patching medical devices, which are unique compared to traditional general computing and IT managed systems.

| FDA Regulatory Requirements | • HDOs typically can not install security patches without manufacturer approval (this could constitute a regulatory violation and create an adulterated device).  
• Manufacturer timelines for evaluating patches often does not align with HDO’s policy to patch within 30/60/etc. days of COTS patch release. |
|----------------------------|-------------------------------------------------------------------------------------------------|
| Limited manufacturer approval of patches | • Few medical device manufacturers today provide routine review and approval for operating system security patches.  
• Even fewer have defined repeatable service level agreements |
| Automated Distribution | • Larger Health Care Delivery Organizations typically rely on automated patch management systems to coordinate the distribution and installation of Operating System updates.  
• Management or security ‘add-on’ agents are generally not approved for use by medical device manufacturers.  
• Complex policies may lead to accidental patching of critical systems |
| Patient Care & Patient Safety | • HDOs have difficulty monitoring for and assessing impact of vulnerabilities and decide on the appropriate action and level of compensating controls  
• Many devices can only be patched when not in-use or in-service |
| Change management and Logistics | • Patches can only be installed during a defined change window  
• Can leverage the existing preventative maintenance cycle for certain devices  
• Version dependency across connected devices may require that multiple end-points be patched simultaneously to prevent backwards incompatibility |
For an HDO to successfully run a patch management program for medical devices, key prerequisites must be met.

**1. Inventory Asset Management**

- Ensure collection of appropriate device asset data
  - I. Inventory
  - II. Discovery
  - III. Maintain IT Asset Profile

**2. Device Risk Profile**

- Triage by Exposure, Likelihood & Impact
  - I. Network Exposure
  - II. Data Exposure
  - III. Patient Safety and Clinical Care Risk
  - IV. Tools & methodologies that can be used

**3. Patch Planning and Execution**

- Validate approval and Safely deploy patch
  - I. Manufacturer Approval
  - II. Validation Testing
  - III. Schedule Patch during Maintenance Cycle
  - IV. ‘Device in-use’ Safeguards
  - V. Deploy and Apply Patch
  - VI. Validate device ready to return to service
In order to properly manage and risk profile medical devices, it is important to gather and maintain the appropriate data. Use automated tools where possible augment with physical discovery.

**Connected? (YES/NO)**
- Host Name / DNS Name
- MAC Address
- IP Address / DHCP
- Wireless Interfaces
- Component wireless

**Operating System**
- OS Version
- OS Patch Level
- Last update date
- List of installed patches
- COTS Middleware
- Application Dependencies

**Safeguards & Capabilities**
- Authentication Controls
- Credential Management
- Anti-Malware or other security technology
- Encryption
- Event alerts and logging
- Remote Access

**Collect MDS2**
**Utilize MDISS MDRAP**
Device Risk Profile

In large environments it is important to prioritize high risk systems. These systems should receive first consideration for application of security patches, vendor engagement and when patching is not feasible, the application of compensating, alternative controls.

Triage by Exposure, Likelihood & Impact

Exposure Considerations:…

- Network Exposure
  - Is the device in an internet accessible network zone
  - Does the device have remote access or phone-home capabilities
    - Consider all methods of remote access (HDO managed (i.e. Token based VPN, B2B Affiliate VPN) and Device Native Phone Home (HTTP/HTTPS Egress Initiated))

- Data Exposure
  - Does the device store sensitive records (PII/PHI)
  - Is the sensitive data transient or permanent
  - What the volume and nature of the records stored

- Patient Safety and Clinical Care Risk
  - Is the device critical to care
  - Is the device life critical or life sustaining
  - Does the device represent a single point of failure

- Has a Device Security Evaluation been performed
  - MDS2
  - MDISS MDRAP
  - Security Architecture and Control Evaluation
Patch Planning and Execution

It is paramount to maintain consideration of regulatory guidelines, manufacturer approval and safe and effective deployment of security patches.

- Obtain Manufacturer Approval
  - Does the Manufacturer have an existing patch management approval service as part of their post-sale maintenance and support process? What is the SLA
  - Obtain list of manufacturer approved patches
    Test patch deployment and documentation (test environment or controlled deployment)

- Only approved patches to deploy
  - Ensure Patch Management system can isolate authorized patches by make/model/device
  - Ensure only authorized and approved patches are configured to deploy to given medical device

- Change Management Considerations
  - Schedule Patch during Preventative Maintenance Cycle, when possible
  - Perform test installation (technical, functional, documentation) as appropriate

Employee ‘Device in-use’ Safeguards

- Ensure two-man rule – so that device is confirmed to be out of service
- Isolate medical device patch management system and devices into ‘maintained VLAN’
- Deploy and Apply Patch
- Validate device ready to return to service
**Patch Management Process Examples**

*High-level process diagram…*

1. **Inventory Asset Management**
   - Develop Asset Profile Requirements
   - Perform Inventory / Discovery
   - Manage Asset Profile

2. **Device Risk Profile**
   - Security Risk Profile
   - Prioritize
   - Control Evaluation
   - Patch Feasible
     - Engage Manufacturer
     - Assess Compensating Controls
     - Manufacturer Authorized Patch?

3. **Patch Planning and Execution**
   - Obtain authorized patch list
   - Isolate Patch by Make/Model
   - Device checked out for service
   - Deploy & Test
   - Reinstate device to service
   - If necessary, deployment in test environment or limited, controlled deployment
Tactical measures to limit risk exposure

In the current environment, patch management of all medical devices may not always be an option. Alternative and complementary controls should be evaluated.

What makes a medical device unique from a general computing device

<table>
<thead>
<tr>
<th>Limited and defined network communication partners</th>
<th>Limited and defined applications and system processes</th>
<th>Functionality limited to the intended use of the device</th>
</tr>
</thead>
</table>

Technical alternative and complimentary controls to patching

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Total segregation</th>
<th>Traffic control (e.g. remote support)</th>
<th>Dynamic Segmentation / Network Access Control</th>
<th>Host Whitelisting (System Processes and Host Network Firewall)</th>
</tr>
</thead>
</table>

A successful device risk management strategy should take advantage of the unique behaviors and characterizes of the systems being protected, medical devices and hospital networks.

See appendix for details
Elevating Lifecycle Management Pressure
Reduce vulnerability and exposure due to long patch cycles

Host Intrusion Prevention / Detection (HIPS/HIDS):
• Application & Process “whitelisting”
• Process / Port control (network, media)
• Exploit prevention
• Critical file protection
• Event alerts and logging
• Extend EOL OS “lifeline”

Regulated Medical Device:
• Manufacturer approval
• Reduce security risks
• Increase reliability
• Reduce support calls

HDO Opportunity:
• Non-regulated device (fridges, building systems, etc.)
• Platform protection for software devices (e.g. PACS)
• Device-supporting IT systems
• Still advisable to coordinate with manufacturer (contract, warranty, support)
Benefits Realized through a Mature Patch Program

**Satisfaction:**
- Avoid downtime and patient / staff frustration

**Treatment / Clinical:**
- Maintain clinical operations
- Improve patient safety

**Electronic Secure Data:**
- Enable medical device integration while maintaining security and compliance

**Patient Engagement and Population Management:**
- Maintain patient trust

**Savings:**
- Avoid costly downtime, fines, and impact on reputation

## Technology Insights

### Security Control

<table>
<thead>
<tr>
<th>Technology</th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Patch Management</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Windows Software Update Service (WSUS) | • No add-on agent required  
• Simplified manufacturer approval process, because no agent needs approval (individual patches still do) | • Requires existing or net-new WSUS Server  
• May require third party controller product to give advanced functionality  
• Third Party Software may require a unique service account on the medical device |
| Agent Based | • Better control of scheduling and patch execution  
Used by most leading enterprise patch management vendors | • Requires add-on patch management security agent.  
• Few manufacturers have a process to vet new security agents for approval |
| **General** | | |
| | • Network technologies provides detection and/or isolation and can help with malicious activity discovery and limit the impact of an outbreak.  
• Suitable as “add on” fix for legacy devices.  
• Valuable component of a “defense in depth” approach. | • In general, any network based approach will not prevent air-gapped infection (e.g. via USB).  
• Creates complexity, administrative and management overhead. |
| **Network Security Monitoring** | • Can detect changes in environment based on network traffic routing and signature analysis.  
• Can detect remote attack or malicious activity from an infected device.  
• Passive traffic scanning typically does not impact device functionality. | • Can invoke false positives.  
• Limited in detection of “zero day” vulnerabilities.  
• Need to have deep understanding of environment to make monitoring data actionable. |
| **VLAN/ACL** | • Provides isolation of medical devices from general IT systems. | • Can end up with large multitude of VLAN’s  
• ACLs can become difficult to manage over time  
Complexity of ACL management may lead to rules which are either ‘too tight’ or ‘too loose’ |
| **Dynamic Segmentation (Network Access Control)** | • Provides most flexibility and management  
• Provides policy based isolation  
• Newer NAC solutions support Device Assets  
• Profile, which simplifies deployment and supports medical devices which may not be able to take an 802.1x certificate. | • NAC may be expensive and challenging to implement  
• Full industry adoption of NAC has been slow  
• Industry confusion between old agent based NAC and newer dynamic NAC  
NAC device profiling which relies on active scanning may pose an availability risk to medical devices |
| Local Firewall | • Inexpensive  
• Easy to Deploy | • Point Solution  
• Multiple discrete firewalls to manage at the local level |
| Local Isolation Zone | • Centrally Managed  
• Can use leading and next-gen firewall technology | • More Expensive option then local firewall solution |
<table>
<thead>
<tr>
<th>Abuse-Case</th>
<th>Risk</th>
<th>Prefered Safe Guard</th>
<th>Compensating Controls</th>
<th>Procurement Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss/Theft of portable equipment</td>
<td>Data Spill</td>
<td>Data-at-Rest Encryption of sensitive data</td>
<td>• RF-ID</td>
<td>- Fixed Disk Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Lock and Cable</td>
<td>- Removable Media Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Lojack</td>
<td></td>
</tr>
<tr>
<td>Vendor provided wireless access</td>
<td>Spectrum Management</td>
<td>Only utilize HDO Enterprise Access Point</td>
<td>• 802.11x channel # 165</td>
<td>- Utilize HDO Wireless Access points</td>
</tr>
<tr>
<td>point</td>
<td>Unauthorized wireless</td>
<td>• Enforce Wireless Enterprise Authentication</td>
<td>• Low gain: &lt;=11 dbm</td>
<td>- or limit to Channel #165 &lt;=11dbm</td>
</tr>
<tr>
<td></td>
<td>access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unpatched operating system</td>
<td>Availability</td>
<td>Timely Patch Management</td>
<td>Statefull Firewall</td>
<td>- Disable unused ports &amp; services</td>
</tr>
<tr>
<td></td>
<td>Data Spill</td>
<td>• Network Access Control (NAC) / Authorized Device Access</td>
<td></td>
<td>- Harden to CIS baseline</td>
</tr>
<tr>
<td></td>
<td>Patient Saftey</td>
<td>• Hardened Operating System</td>
<td></td>
<td>- Include stateful firewall</td>
</tr>
<tr>
<td>Medical device transmits sensitive data insecurely</td>
<td>Data Spill</td>
<td>Encryption: Data-in-transit</td>
<td>Encryption interface broker, IPSec Switch to Switch</td>
<td>- Validate strong encryption in transit (i.e. SSL/TLS 1.2 or IPSEC</td>
</tr>
<tr>
<td>Medical device vulnerabilities and exploit</td>
<td>Availability</td>
<td>Security evaluation and penetration testing</td>
<td>Statefull Firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Spill</td>
<td>• Local Isolation Zone, VLAN-ACL, or Local Firewall</td>
<td></td>
<td>- Manufacturer to produce MDS(2)</td>
</tr>
<tr>
<td></td>
<td>Patient Saftey</td>
<td>• Security Assessment for remote support &amp; remote diagnostic systems</td>
<td></td>
<td>- Manufacturer to share vulnerability scan report and 3rd party assessments</td>
</tr>
<tr>
<td>Medical Devices phone-home (</td>
<td>No Challenge Access</td>
<td>Local Isolation Zone, VLAN-ACL, or Local Firewall</td>
<td>Next-Gen firewall to block non HTTP traffic on port 80/443</td>
<td>- Encrypted Tunnels</td>
</tr>
<tr>
<td></td>
<td>Unattended Activities</td>
<td>• Pivot to other network resources</td>
<td></td>
<td>- 'Challenge Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Limited access to PHI during remote access session</td>
</tr>
<tr>
<td>Inappropriate access using device</td>
<td>Availability</td>
<td>Manufacturer disclosure of all service accounts</td>
<td>Disclose service accounts, Access Review</td>
<td>- Disable unnecessary accounts</td>
</tr>
<tr>
<td>service accounts</td>
<td>Data Spill</td>
<td>• HDO to change and maintain account passwords</td>
<td></td>
<td>- Document required service, auto-logon and support accounts</td>
</tr>
<tr>
<td></td>
<td>Patient Saftey</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References - FDA

Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and FDA Administration Staff (Jan 2016)

Content of Premarket Submission for Management of Cybersecurity in Medical Devices: Guidance for Industry and FDA Administration Staff (Oct. 2014)

http://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm

Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication (2013)
http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm?source=govdelivery


http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm

Off-The-Shelf Software Use in Medical Devices (Sept. 1999)
http://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf
References - Other

Medical Device Software Patching, IHE PCD in Cooperation with MDISS (Oct. 2015),

Medical Equipment Management, Medical Device Cyber Security Best Practice Guide, IHE PCD

Medical Equipment Management, Cyber Security, IHE PCD (May 2011),

Building Code for Medical Device Software Security, IEEE Computer Society, May 2015,

Medical Device Isolation Architecture Guide, V2.0, US Department of Veterans Affairs (Aug. 2009),

Medical Devices Security Technical Implementation Guide, V1 R1, Defense Information Systems Agency (DISA) (July 2010),

Patching Off-the-Shelf Software Used in Medical Information Systems, NEMA/COCIR/JIRA Security

Manufacturer Disclosure Statement for Medical Device Security, NEMA (Oct. 2013);
http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx
Questions

Speaker Contact Information:

*Ron Mehring*, MBA, CISSP  
Vice President – Technology & Security  
Texas Health Resources  
RonaldMehring@TexasHealth.org

*Axel Wirth*, CPHIMS, CISSP, HCISPP  
Distinguished Solutions Architect,  
US Healthcare Industry  
Symantec Corporation  
Mobile: 617-999-4035  
axel_wirth@symantec.com