Improving patient safety and outcomes through medical device connectivity

College of Healthcare Information Management Executives
CHIME CollegeLive

7 September 2016

Advancing the world of health
Who we are: BD is a leading medical technology company that partners with customers and stakeholders to address many of the world’s most pressing and evolving health needs.
Device interoperability at BD

BD’s Medical Internet of Things

“Link Diagnosis and Care Delivery to Solve Health System Problems and Improve the Lives of Individual Patients”
Purpose

Today’s session examines improvements in patient safety through error prevention, efficient workflows, and improved care documentation, as a result of integrating medical devices with the EHR.

All types of modern medical devices can connect with the EHR. Today we will focus on real-world examples of bi-directional interoperability between wireless infusion pumps and the EHR.

Our goal is to arm you with information to be an active participant as your organization evaluates the return on investment when considering medical device interoperability.
Key definitions

**Medical Device Interoperability**
The ability of the medical device to interact with the electronic health record and other information systems in order to improve patient safety, reduce waste, and enhance functionality.

**Waste**
Any activity that does not add value to the healthcare system.
Recent studies show clinicians see value with connected medical devices

- Change in mindset from a decade ago.
- Nurses want medical devices to integrate with the EHR.
- Nurses agree, coordinated and connected medical device data improves patients safely.
- Half of the nurses said they have witnessed a medical device error.

**Example:** Infusion associated adverse drug events add more than $2 billion to annual healthcare costs*

Interoperability transforms from device-centric, to patient-centric data association

• Promotes formulary standardization,
• Enables CMS charge capture requirements,
• Reduces time wasted on manual documentation,
• Supports accurate EHR data, and
• Associates patient to infusion device.
Demonstrated efficiency, cost and patient benefits
Example of BCMA interoperability workflow at the point-of-care
Scan the patient identification band
Scan the medication bag or syringe
Scan the pump
Confirm medication order and start
Automatically verifies running infusion matches order
Integrating the Healthcare Enterprise (IHE) is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as HL7 to address specific clinical need in support of optimal patient care.
IHE Patient Care Domain (PCD) profiles allow scale and repeatable implementations.

Using HL/7 standards and IHE Profiles minimize EHR data mapping and interface requirements.
Lessons learned – it’s more than technology alone

Example:
- Master formulary must line-up with infusion pump internal medication library database.
- Device manufacturers must provide resources and support aligned to enterprise HIT System environments.
Managing and securing connected medical devices

Traditional methods may not work
Medical devices are regulated

- Medical device vendors register and obtain approval to manufacture and market globally.
- FDA is the regulatory agency for medical devices in the United States.
- Data-centric medical device manufacturers also need to factor in HIPAA considerations and BAA requirements.
- Policy and procedures that work for existing networked technologies might conflict with regulatory requirements.
What does this mean for software updates and security patches

- FDA requires device manufacturers submit for pre-approval if any software updates (including patches) change the intended use or raises new issues regarding safety of the device.
- For normal security patching, pre-approvals are rare.
- The device manufacturer will verify all patches to intended use claims and safety requirements before release. Some cases may cause delays but still must remain aligned with hospital IT practice.
High-level view of medical devices in a common security infrastructure required to support both regulated and unregulated devices and applications.
Detailed look at architecture

- Text in red are regulated systems.
- Although on a common platform, the regulated components may require adjustments to policy and procedures in order to support and manage.
Patient safety and product security is Priority #1

Organization requirements at BD to support security across all platforms and devices
Medical device security challenges

- Medical devices ‘act’ differently but must be secure and efficient on the network.
- Many medical devices do not incorporate Commercial Off The Shelf (COTS) operating systems so a different set of rules apply.
- Authentication is typically performed at the device not the user (nurses do not logon to infusion pumps).
Questions to ask

<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical scope</td>
<td>Are large-volume and syringe pumps integrated with the EHR today?</td>
</tr>
<tr>
<td></td>
<td>Does the infusion pump continue to protect the patient using SHF after the initial auto programming once with complex multi-ingredient medications?</td>
</tr>
<tr>
<td>Technical platform</td>
<td>What communication method does the system use to optimize bandwidth utilization and minimize TCP overhead issues?</td>
</tr>
<tr>
<td></td>
<td>Does the system provide fail-overing?</td>
</tr>
<tr>
<td></td>
<td>What are the average latency times from the pump programming?</td>
</tr>
<tr>
<td></td>
<td>Can the platform support your entire enterprise through a single interface on a single server?</td>
</tr>
<tr>
<td></td>
<td>Can both large-volume and syringe pumps be integrated with this EHR in a single implementation?</td>
</tr>
<tr>
<td></td>
<td>Has a qualified third-party validated commercial security technology and procedures?</td>
</tr>
<tr>
<td></td>
<td>Will the pump limit RF output to a pump-device to lowest power necessary?</td>
</tr>
<tr>
<td></td>
<td>Did the infusion system vendor implement server hardening techniques? How?</td>
</tr>
<tr>
<td></td>
<td>Will the pumps function clinically and perform &quot;store and forward&quot; in the event of network disruption?</td>
</tr>
<tr>
<td></td>
<td>Will the infusion system leverage existing hospital Active Directory services?</td>
</tr>
<tr>
<td></td>
<td>Can your infusion solution support multiple types of basalities and checklists to share a single, second, wireless connection?</td>
</tr>
<tr>
<td></td>
<td>Does your infusion platform vendor validated wireless claims with on-site testing?</td>
</tr>
<tr>
<td>Sustaining support</td>
<td>Will the infusion system vendor provide 24/7 remote error health monitoring?</td>
</tr>
<tr>
<td></td>
<td>Is support personnel available on third-party personnel?</td>
</tr>
<tr>
<td></td>
<td>How many of the vendor’s infusion pumps have already been installed and operational?</td>
</tr>
<tr>
<td></td>
<td>How many are integrated with EMR and HIS?</td>
</tr>
<tr>
<td></td>
<td>Will the infusion vendor supply expert resource as part of the implementation in project management, personnel management, nurse workflow, IT integration and clinical engineering?</td>
</tr>
</tbody>
</table>

- Evaluating connected medical devices will require a unique set of criteria.
- Currently only government hospitals require FIPS 140-2 Wireless Certification by NIST.
- New programs underway at NIST and the FDA regarding infusion wireless security certification.
- HIMSS and the National Electrical Manufacturers Association’s Statement for Medical Device Security (MDS²) and ANSI/AAMI/ IEC 80001 Risk Assessment Standards are good starting points in evaluating device security risks.
- The sheer number of possible devices should also include requirements for bandwidth consumption and latency delays.
# Technical responsibilities

Managing medical devices is a collaborative process

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Vendor</th>
<th>Hospital IT</th>
<th>Hospital BioMed</th>
<th>Comments</th>
</tr>
</thead>
</table>
| Evaluate device security     | ✔      | ✔           |                 | - Patient privacy  
- Breach protection  
- Device control protection  
- Hospital policies                                                                                                                     |
| capabilities                 |        |             |                 |                                                                                                                                          |
| Evaluate device for repair   | ✔      | ✔           | ✔               | Traditionally a stand-alone Biomedical responsibility. Hospital IT may need to evaluate wireless and server infrastructure as part of the process |
| and sustainability           |        |             |                 |                                                                                                                                          |
| Remote management            | ✔      | ✔           |                 | Surveillance for embedded medical devices and how the remote link is secure                                                                |
| Network consumption          | ✔      | ✔           |                 | Sheer numbers of networked medical devices require proper stewardship of infrastructure resources                                          |
| Patch management             | ✔      | ✔           |                 | Vendor may need to validate patch prior to installation. Installation may be done by hospital IT, the vendor (remotely), or both          |
| Device configuration         | ✔      | ✔           | ✔               | Hospital IT for network configurations  
Hospital Biomedical for clinical configuration                                                                                             |
| Device break-and-fix         | ✔      |             | ✔               | Hospital Biomedical is qualified to manage repairs                                                                                        |
| Problem resolution           | ✔      | ✔           | ✔               | Connected medical devices are performing a clinical function in near real-time 24hr/day. Problems may require assessment from Biomedical, IT, and the vendor to resolve. |
| More ….                     | ✔      | ✔           | ✔               |                                                                                                                                          |
Act differently

- Healthcare continues to transform itself.
- Legacy medical device manufacturers will also need to transform to meet these new data centric opportunities.
What does this all mean?

• Healthcare IT needs to be directly engaged when evaluating these new data-centric connected medical devices.
• Device vendors need to better understand the complexities and risk of connecting to the hospital network infrastructure.
• CIO’s must think differently about connected medical devices.
• By design, many medical devices do not incorporate COTS and will require modified procedures for patching and updates.
• Training and organization accountability will be key to integrate and take full advantage of medical device interoperability.
Where can we go from here

Moving towards a common infrastructure should accelerate regulated medical device connectivity across the continuum of care.
Lessons learned and best practice

• Medical device integration is a collaborative process
  – Device security and data integration development continue to evolve.
  – Device manufacturers, Hospital IT & Biomed, and clinical, need to work together in order to take advantage of a secure connected medical device system.

• Best practice suggests:
  – Understand that the total project scope is more than technology alone.
  – Develop evaluation and security procedures to handle regulated connected devices that may not incorporate COTS.
  – Evaluate effort and ROI based on both EHR and enterprise device capabilities.
  – Promote organizational changes and cross-training; harmonizing Biomedical and IT support functions.
  – Require device manufacturers to scale and support enterprise EHR connectivity.

*It is worth the effort*
Questions