AHA and Cybersecurity

- Member education
- Coordination with federal government
- Policy
Policy Approaches

- Medical devices are a key vulnerability
- Fraud and abuse laws stand in the way
- Better balance of information sharing and security
- Interaction with HIPAA
- Workforce and resource challenges
Role of the FDA

FDA Guidance and Roles
- Pre-market
- Post-market
- Assistance during attack

Recent AHA Recommendations
“The FDA must provide greater oversight of medical device manufacturers with respect to the security of their products. Manufacturers must be held accountable to proactively minimize risk and continue updating and patching devices as new intelligence and threats emerge.

“We recommend that the FDA proactively set clear, measurable expectations for manufacturers before incidents and play a more active role during cybersecurity attacks. This active role could include, for example, issuing guidance to manufacturers outlining the expectations for supporting their customers to secure their products.”
Laura Hars

Senior Manager, Cyber
BDO Advisory Services
Overview

• Introduction to medical device risk
• What can go wrong?
• Compliance
Medical Devices

- What Are They?
- What Types?
Wireless Implantable Medical Devices

- Deep Brain Neurostimulators
- Cochlear Implants
- Cardiac Defibrillators/Pacemakers
- Gastric Stimulators
- Foot Drop Implants
- Insulin Pumps

Image Credit: Massachusetts Institute of Technology
Cybersecurity & Medical Devices

Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post-market cybersecurity guidance provide recommendations for meeting QSRs.
Biggest Challenges of Securing Medical Devices

What do you think is the biggest challenge facing the medical device industry with regards to cybersecurity?

Votes received: 502

- Identifying and mitigating the risks of fielded and legacy devices: 30.1%
- Embedding vulnerability management into the design phase of medical devices: 19.7%
- Meeting regulatory requirements: 8.4%
- Lack of collaboration on cyber threat management throughout connected medical device supply chain: 17.9%
- Monitoring and responding to cybersecurity incidents: 19.5%

4.4% Don’t know/Not applicable
Differences in Impact of Failure

Security (i.e., data confidentiality, integrity or availability) compromise can
✓ have serious financial impact
✓ have serious operational impact
✓ have serious reputation & legal impact

Security compromise of Medical Devices can result in death or serious injury
Information Technology vs Clinical/Biomedical Engineering

IT knows data security

BUT ...
IT generally has limited knowledge of type, number and vulnerabilities associated with medical devices

CE knows number/location of medical devices & misunderstands criticality, lifecycle, and supportability issues

BUT ...
CE generally has limited knowledge of data security issues
Medical Devices & Systems: Shared Responsibility

Degree of Integrated Support

Currently 40% Networked (and rapidly growing)

Still significant disconnect … resulting in coverage gaps

Overlapping Responsibility?

CLINICAL / BIOMEDICAL ENGINEERING

INFORMATION TECHNOLOGY
Case Study – Medical Device Concerns at a Large Healthcare Provider Network

During a cybersecurity assessment the following concerns were noted:

- The IT department estimated the number of devices on the network to be approximately 61,000 based on the current asset inventory
- A scan of the network revealed slightly over 98,000 devices
- Through interviews with clinical personnel and examinations of manual inventories, it was determined that approximately 35,000 of the 98,000 devices were medical devices (infusion pumps, pacemakers etc.)
- The Clinical Engineering department maintained an inventory of device manufacturers and serial numbers of the devices but not their network address
- Although the IT department had to be contacted to enable the connectivity of the device on the hospital network, they also did not keep any inventory or notation of the devices network address

Solution:
The issue of tracking medical devices was solved by creating a business process that involved both departments using the IT Service Desk tool to track and record the purchase and registration of the devices on the network
FDA Guidance on Responsibility – Manufacturers vs Providers

Cyber Risk

The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.

The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.

“Cybersecurity routine updates and patches,” are generally considered to be a type of device enhancement for which the FDA does not require advance notification or reporting under 21 CFR part 806.
Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.

The FDA recognizes that Health care Delivery Organizations (HDOs) are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.
Controlled Versus Uncontrolled Risk

Threat x Vulnerability x Consequence = Risk
Steps to Cybersecurity for Internet of Things - Medical Devices

1. Categorize existing devices based on risk
2. Implement a clinical risk management framework
3. Ensure your organization follows basic security hygiene
4. Include security requirements in new device contracts or requests for proposals
5. Apply a zero trust networking architecture
Questions?
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, Dec. 12, 2017</td>
<td>3-4 pm ET</td>
<td>Responding in Times of Crisis: Incident Response and Cyber Threat Intelligence</td>
</tr>
<tr>
<td>Tuesday, Jan 9, 2018</td>
<td>3-4 pm ET</td>
<td>Risk Management: Assessing Your Cybersecurity Program and Promoting a Culture of Cybersecurity</td>
</tr>
<tr>
<td>Tuesday, Jan 23, 2018</td>
<td>3-4 pm ET</td>
<td>Medical Devices and Cyber Issues</td>
</tr>
<tr>
<td>Tuesday, Feb 6, 2018</td>
<td>3-4 pm ET</td>
<td>Cyber Incident Exercise: The Roles of Hospital Leaders</td>
</tr>
<tr>
<td>Tuesday, Feb 20, 2018</td>
<td>3-4 pm ET</td>
<td>Bringing it All Together: Key Take-Aways</td>
</tr>
</tbody>
</table>

Register at: www.aha.org/cybersecurity
Laura Hars
Senior Manager
Cybersecurity
BDO Advisory Services
Direct: +1 732 734-3059
Mobile: +1 973 903-0453
Email: Lhars@bdo.com
BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO’s global network of more than 67,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm’s individual needs.