The Evolving State of Medical Device Cybersecurity
Session 16, February 20, 2017

Seth Carmody, FDA CDRH, Cyber Security Program Manager
Margie Zuk, Senior Principal Cybersecurity Engineer, The MITRE Corporation
Speaker Introduction

Seth Carmody, PhD.
Cyber Security Program Manager
FDA Center for Devices and Radiologic Health

Margie Zuk, B.S., M.S.
Senior Principal Cybersecurity Engineer
The MITRE Corporation
Conflict of Interest

Seth Carmody, FDA CDRH, PhD.
Margie Zuk, MITRE, B.S., M.S.

Have no real or apparent conflicts of interest to report.
Medical device cybersecurity is a complex ecosystem challenge.

The FDA’s recently released final guidance on postmarket management of cybersecurity in medical devices is part of the FDA’s ongoing efforts to ensure the safety and effectiveness of medical devices as they face potential cyber threats, at all stages in the device’s lifecycle.

The ecosystem is rapidly evolving and numerous collaborative efforts are proactively addressing cybersecurity risks in medical devices in order to keep patients safe.
Agenda

• The Medical Device Cybersecurity Challenge
• FDA and Cybersecurity
• The Medical Device Cybersecurity Ecosystem
• Evolving Ecosystem Efforts
Learning Objectives

• Describe the FDA’s Final Postmarket Management of Cybersecurity in Medical Devices, to include the main policy tenets FDA has put forward that address security throughout the total product lifecycle

• Identify the current medical device cybersecurity ecosystem gaps and discuss progress made and/or underway to close these gaps

• Recognize the evolving medical device cybersecurity ecosystem to include many emerging efforts and their role within the larger healthcare cybersecurity ecosystem
Realizing the Value of Health IT

**Improve Patient Safety**
Through coordinated disclosure and vulnerability sharing

**Reduce the # of PHI Breaches**
Through improved medical device cybersecurity vulnerability management

**Reduce the # of PHI Breaches**
Through improved medical device cybersecurity vulnerability management
Medical Device Characteristics

• Increasingly rely upon **computers, software, and networking**

• Often incorporate **third-party software**

• Are subject to **regulation**, therefore FDA guidance serves as policy framework to enable patching and reconfiguration, if appropriate

• Historically were designed **without secure development techniques**
Medical Devices in the Clinical Environment

• The health care and public health (HPH) critical infrastructure sector represents a significantly large attack surface for national security today

• Connected medical devices, like all other computer systems, incorporate software that are vulnerable to threats

• We are aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations

• When medical device vulnerabilities are not addressed and remediated, they can serve as access points for entry into hospital/health care facility networks
Incidents & Researcher-Demonstrated Examples

“Hacking” of implantable insulin pump (Radcliffe, 8/11)

Security researchers present FDA with cyber vulnerabilities of medical devices due to hardcoded passwords (Rios & McCorkle, 4/13)

Vulnerabilities identified in PCA and other Infusion Pumps (Rios, 5/14-6/15)

Vulnerabilities identified in Animas OneTouch Ping insulin pumps by Johnson & Johnson (Rapid7, Oct 2016)

Vulnerabilities in BD/CareFusion Pyxis Supply Station (Rios/Ahmadi, March 2016)
Executive Efforts to Strengthen Critical Infrastructure Cybersecurity

**Presidential Policy Directive 8 (PPD-8):** National Preparedness Post-Katrina: “federal departments and agencies to work with the whole community to develop a national preparedness goal and a series of frameworks and plans related to reaching specified goals.”

**PPD-21:** Critical Infrastructure Security and Resilience

**Executive Order 13636:** Improving Critical Infrastructure Cybersecurity a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure

**NIST Cybersecurity Framework:** Voluntary risk-based framework to help organizations manage cyber risk

**Executive Order 13691:** Promoting Private Sector Cybersecurity Information Sharing
FDA Goals

• Meet our mission: safe and effective devices
• Raise cybersecurity awareness
• Promote safety and security by design through establishing clear regulatory expectations
• Promote coordinated vulnerability disclosure & proactive vulnerability management
• Minimize reactive approaches
• Foster ‘whole of community’ approach
## Timeline of Key FDA Activities

<table>
<thead>
<tr>
<th>Year</th>
<th>Activities</th>
</tr>
</thead>
</table>
| 2013 | Began coordination with Department Homeland Security Industrial Control Systems Cyber Emergency Response Team (DHS-ICS-CERT) in response to security researchers reporting of vulnerabilities  
Issued Safety Communication on shared ownership and shared responsibility among stakeholders, cyber hygiene  
Engaged in outreach, education, and building collaboration |
| 2014 | Executed Memorandum of Understanding with the National Health Information Sharing & Analysis Center (NH-ISAC)  
Final Premarket Cybersecurity Guidance Released  
Convened workshop, ‘Collaborative Approaches for Medical Device and Healthcare Cybersecurity’ |
| 2015 | Ongoing coordination with DHS-ICS-CERT, medical device manufacturers and security researchers on reported medical device vulnerabilities  
Fostered collaboration with multiple stakeholder groups across the ecosystem  
Issued product-specific safety communications on medical device vulnerabilities |
| 2016 | Draft Postmarket Cybersecurity Guidance Released  
Convened workshop, ‘Moving Forward: Collaborative Approaches for Medical Device and Healthcare Cybersecurity’  
Final Postmarket Cybersecurity Guidance Released |
FDA Public Workshops: Collaborative Approaches to Medical Device Cybersecurity

• Goals:
  • Catalyze collaboration among all Healthcare and Public Health sector stakeholders
  • Identify barriers that impede efforts towards promoting cybersecurity
  • Advance the discussion on innovative approaches for building securable medical devices

• First workshop October 21-22 2014
  • Co-sponsored with HHS and DHS

• Second workshop January 20-21 2016
  • Co-sponsored with NH-ISAC, HHS and DHS

• Broad range of stakeholders
Key Principles of FDA Premarket Cybersecurity Guidance

• Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
• Address cybersecurity during the design and development of the medical device
• Establish design inputs for device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)
Key Principles of FDA Post Market Cybersecurity Guidance

• Collaborative approach to information sharing and risk assessment
• Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities
• Align with Presidential EOs and NIST Framework
• Incentivize the “right” behavior
• Risk-based approach to assuring risks to public health are addressed in a timely fashion

*To view the final guidance webinar visit: [http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm](http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm)
FDA Post Market Cybersecurity Guidance: What’s Changed

• Policy unchanged

• Clarifications include:
  – Terminology now consistent with FDA-recognized standards
  – Definition and criteria for active participation with ISAOs
  – Scope of guidance with respect to privacy and confidentiality harms

• Modification of 30 day remediation timeframe has been expanded to include a 60 day tier
Medical Device Cybersecurity Risk Management

- Assessing Exploitability of the Cybersecurity Vulnerability
- Assessing Severity of Patient Harm
- Evaluation of Risk to Safety and Essential Performance
Key Medical Device Cybersecurity Myth Busters

- Myth: Manufacturers are not permitted to make updates to devices for cybersecurity without going back to FDA first for “re-certification”

- Fact: Most medical device software changes made solely to strengthen cybersecurity do not require pre-market review or product recall (there are some exceptions).

- Myth: Cybersecurity of medical devices is voluntary for medical device manufacturers and not enforceable.

- Fact: Medical device manufacturers are required by law to comply with all applicable regulations, including the quality system regulations (QSRs). The pre- and post-market cybersecurity guidances articulate that a comprehensive, structured and systematic cybersecurity risk management program is necessary under the Quality System Regulation.
FDA and CAMH*

• MITRE helping to advance the FDA medical device cybersecurity vision
  – Medical device cybersecurity stakeholder engagement study and gap analysis
  – Tailoring the Common Vulnerability Scoring System for healthcare
  – Participating in medical device vulnerability and threat information sharing activities

* CMS Alliance for Healthcare Modernization (CAMH) is a Federally Funded Research and Development Center operated by The MITRE Corporation
Medical Device Ecosystem
Gap Areas

• Need to share best practices for securing legacy devices
• Need to adopt threat based defense and sharing of threat intelligence
• Need coordinated disclosure of vulnerabilities and transparency of vulnerabilities in third party software
• Need cybersecurity solutions for large and small organizations
• Need a common risk framework for security and safety
• Need cybersecurity baselines for medical devices
• Need cybersecurity testing/certification of medical devices
• Need a systems engineering view across the lifecycle
• Need to develop integrated cyber and physical preparedness and response plans
• Need to develop incentives and business cases
Evolving Ecosystem Efforts

• Healthcare Industry Cybersecurity Task Force
• Information Sharing and Analysis Organizations and Centers
• Medical Device Cybersecurity Standards and Guidance
• Medical Device Testing and Certification
• CVSS for Healthcare
• Coordinated Vulnerability Disclosure
• Bill of Materials
Healthcare Industry Cybersecurity Task Force Responsibilities

• Analyzing how other industries have implemented strategies and safeguards to address cybersecurity threats.
• Analyzing challenges and barriers the health care industry encounters when securing itself against cyber attacks.
• Reviewing challenges to secure networked medical devices and other software or systems that connect to an electronic health record.
• Providing the Secretary with information to disseminate to health care industry stakeholders to improve their preparedness for, and response to, cybersecurity threats.
• Establishing a plan to create a single system for the Federal Government to share actionable intelligence regarding cybersecurity threats to the health care industry in near real time for no fee.
• Reporting to Congress on the findings and recommendations of the task force
National Health ISAC/MDISS Partnership

- Established Medical Device Security Information Sharing Council
- Signed MOU with FDA around collaboration of Medical Device Cybersecurity in October 2016
- Convening regional medical device security workshops
  - Conducted 4 workshops in 2016
  - 7 currently planned for 2017
- Medical device track at NH-ISAC Summits
- Implementing medical device information sharing initiatives
  - MDRAP, MDSATI, MDVISI
National Cybersecurity Center of Excellence

**Mission:** Collaborate with innovators to provide standards-based cybersecurity capabilities that address today’s business needs

- Partnership among industry, academics and government

- Example solutions to businesses’ most pressing cybersecurity challenges in health and other sectors of the U.S. economy
  - Securing Wireless Infusion Pumps – draft out Aug 2016
  - Data Integrity – white paper published Dec 2015
Diabetes Technology Society

• Public release of cybersecurity standard in May, 2016 to raise confidence in the security of networked medical devices through independent expert security evaluation
  – Leverages ISO/IEC 15408
  – Targets networked life critical devices
    • Initially targets diabetes devices but could be used for evaluation of other devices in the broader internet of things
  – Approved 2 evaluation labs (Brightsight and Booz Allen Hamilton)
• MEDSec: Security and Privacy for the Internet of Medical Things (May 2016, May 2017)
  – Medical device cybersecurity conference that brings together regulators, manufacturers, hardware and software suppliers, ethical hackers, and legal experts
Underwriters Laboratories (UL)  
Cybersecurity Assurance Program (CAP)

- UL CAP offers trusted third party support for evaluating the security of network-connectable systems and vendor processes for developing and maintaining systems with a focus on security

- Tailoring UL2900 series of standards for medical devices

- UL2900 can be evaluated through fuzz testing to identify zero days, evaluate known vulnerabilities that haven’t been patched, identify known malware, static source code and binary analysis, use of specific security controls, structured penetration testing, risk assessment of security mitigations

- In June, 2016 UL entered into a CRADA with VA to improve cybersecurity standards and certification approaches for medical devices through the CAP
Common Vulnerability Scoring System for Medical Devices

- CVSS is an open framework developed by the Forum of Incident Response and Security Teams (FIRST) for communicating the characteristics and severity of software vulnerabilities
- CVSS scores often sensationalize medical device vulnerabilities by not taking into account the clinical environment
- Formed a working group, including medical device manufacturers, healthcare providers, and cybersecurity experts to develop an approach for using CVSS to score medical device vulnerabilities
  - Develop guidance/rubric
  - Recommend potential modifications
Coordinated Vulnerability Disclosure

• ISO/IEC 29147 (Information technology – Security techniques – Vulnerability disclosure) made available at no cost

• I am the Cavalry tracking evolving disclosure policies:
  • Siemens
  • Philips
  • Medtronic
  • Draeger
  • Abbott
  • GE
  • Johnson & Johnson
  • St. Jude Medical
  • Orion Health
Bill of Materials

• Need for transparency of third-party software components for medical devices to track vulnerabilities
  – Enables healthcare providers to assess the risk of medical devices on their networks
  – Enables healthcare providers to implement mitigation strategies when patches are not available
• Limited adoption of this practice
  – Royal Philips – May 2016
Realizing the Value of Health IT

Improve Patient Safety
Through coordinated disclosure and vulnerability sharing

Reduce the # of PHI Breaches
Through improved medical device cybersecurity vulnerability management
Key Messages

• Medical device cybersecurity is a complex ecosystem challenge

• The FDA’s recently released final guidance on postmarket management of cybersecurity in medical devices is part of the FDA’s ongoing efforts to ensure the safety and effectiveness of medical devices as they face potential cyber threats, at all stages in the device’s lifecycle

• The ecosystem is rapidly evolving and numerous collaborative efforts are proactively addressing cybersecurity risks in medical devices in order to keep patients safe
Questions

• Seth Carmody, FDA
  Seth.Carmody@fda.hhs.gov

• Margie Zuk, MITRE
  mmz@mitre.org

For more information, visit the Federal Health IT Pavilion