MEDICAL DEVICE CYBERSECURITY

SETH D CARMODY PHD
APRIL 4, 2018
15TH ANNUAL MEDICAL DEVICE QUALITY CONGRESS
Framing The Issue: Environment

• The health care and public health (HPH) critical infrastructure sector represents a significantly large attack surface for national security today
  – Intrusions and breaches occur through weaknesses in the system architecture

• 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
  – May lead to compromise of data confidentiality, integrity, and availability
Executive Orders (EO), Presidential Policy Directives, and Framework to Strengthen Critical Infrastructure Cybersecurity

- EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” May 17, 2017
- EO 13636 (Feb 2013) → NIST Voluntary Framework (Feb 2014) v1.1 in Draft Jan. 10, 2017
- PPD 21 (Feb 2013)
- EO 13691 (Feb 2015) – establishment of Information Sharing and Analysis Organizations (ISAO)
A Complex Ecosystem

Medical Device Ecosystem

- Industry
- Professional Societies
- Regulators
- Payers
- Health Care Providers
- Patients
- Venture Capitalists
- Researchers

www.fda.gov
Let’s Play: Fact vs. Myth

Fact vs. Myth

The FDA is the federal entity solely responsible for the cybersecurity of medical devices.

Fact: The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, healthcare delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.

www.fda.gov
What is Security?

“... software engineering is about ensuring that certain things happen ..., security is about ensuring that they don’t”

Bricks are Safe

Until Thrown...

Intended Use + Misuse


Negative Requirements are *Infinite*!

**Features:**
What a Device **MUST Do**...
Get drug libraries from the Internet

**Safety:**
What a Device **MUST NOT** do
Thou, shall not under or over deliver therapy!

*Hackerman – Movie, Kung Fury 2015*
Let’s Play: Fact vs. Myth

**Fact** vs. **Myth**

Cybersecurity for medical devices is optional.

**Myth**

**FACT:** 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 guidances provide recommendations for meeting QSRs.
Premarket Cybersecurity Guidance

• Draft June 2013
• Final October 2014
• Key Principles:
  – #1 Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
  – #2 Address cybersecurity during the design and development of the medical device
  – #3 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)
Let’s Play: Fact vs. Myth

**Fact vs. Myth**

The FDA does not conduct premarket testing for any medical products.

FACT

**Myth:** The FDA tests for cybersecurity of medical devices.
Key Principles of FDA Postmarket Management of Cybersecurity in Medical Devices

• Use a risk-based framework to assure risks to public health are addressed in a continual and timely fashion
• Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities
• Foster a collaborative and coordinated approach to information sharing and risk assessment
• Align with Presidential EOs and NIST Framework
• Incentivize the “right” behavior
Let’s Play: Fact vs. Myth

Fact vs. Myth

Medical device manufacturers can’t update medical devices for cybersecurity.

Myth

FACT: 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

www.fda.gov
Let’s Play: Fact vs. Myth

Fact vs. Myth
Health care Delivery Organizations (HDOs) can’t update and patch medical devices for cybersecurity.

Myth

Fact: The FDA recognizes that 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.
Cybersecurity – Assessing Risk

Assessment of impact of vulnerability on safety and essential performance of the medical device based on:

• Severity of Patient Harm (if the vulnerability were to be exploited)
• Exploitability
Key Terms: Safety and Essential Performance

- Derived from American National Standards Institute/Association for the Advancement of Medical Instrumentation (ANSI/AAMI) ES60601-1: Medical electrical equipment—Part 1: General requirements for basic safety and essential performance.

- Functions of a device which must remain operational in order to fulfill the intended use and that can be disrupted by exploit.
Key Term: Patient Harm

- Derived from ANSI/AAMI/ISO 14971: Medical Devices – Application of Risk Management to Medical Devices
- Limited scope to physical harm to patients
  - Changes to devices to address uncontrolled risk of patient harm are called remediations
- Changes to devices to address controlled risk of patient harm and/or other harms would be categorized as cybersecurity routine updates and patches
Postmarket Cybersecurity Risk Assessment

Severity of Patient Harm (if exploited)

Negligible  Minor  Serious  Critical  Catastrophic

Exploitability

High  Medium  Low

Uncontrolled Risk

Controlled Risk
Assessing Exploitability with Common Vulnerability Scoring System (CVSS)

- Establish a repeatable process by leveraging existing frameworks (e.g. CVSS)

**Base Scoring (risk factors of the vulnerability)**
e.g. Attack Vector (physical, local, adjacent, network)

**Temporal Scoring (risk factors that change over time)**
e.g. Exploit Code Maturity (high, functional, proof-of-concept, unproven)

**Environmental scoring (controls that reduce risk)**
e.g. Physical, software, network, compensating controls.

CVSS – Common Vulnerability Scoring System [https://www.first.org/cvss](https://www.first.org/cvss)
### Assessing Severity

<table>
<thead>
<tr>
<th>Common Term</th>
<th>Possible Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Inconvenience or temporary discomfort</td>
</tr>
<tr>
<td>Minor</td>
<td>Results in temporary injury or impairment not requiring professional medical intervention</td>
</tr>
<tr>
<td>Serious</td>
<td>Results in injury or impairment requiring professional medical intervention</td>
</tr>
<tr>
<td>Critical</td>
<td>Results in permanent impairment or life-threatening injury</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Results in patient death</td>
</tr>
</tbody>
</table>

ANSI/AAMI/ISO 14971: 2007/(R)2010: Medical Devices – Application of Risk Management to Medical Devices:
Changes to a Device for Controlled vs. Uncontrolled Risk

Risk of patient harm

Yes

Controlled

Changes are Cybersecurity routine updates and patches, device enhancements

Uncontrolled

Meet three criteria:
1. No adverse events
2. Remediate within timeline
3. Active participant in an ISAO

No

Changes are Cybersecurity routine updates and patches, device enhancements

Yes

806 report (Reports of Corrections and Removals) not required

No

806 report required

Distinguishing Medical Device Recalls from Medical Device Enhancements

ISAO (Information Sharing and Analysis Organization)
Information Sharing and Analysis Organizations (ISAO) – What are they?

The ISAO best practice models are intended to be:

**Inclusive** - groups from any and all sectors, both non-profit and for-profit, expert or novice, should be able to participate in an ISAO;

**Actionable** - groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO;

**Transparent** - groups interested in an ISAO model will have adequate understanding of how that model operates and if it meets their needs; and

**Trusted** - participants in an ISAO can request that their information be treated as [Protected Critical Infrastructure Information](#). Such information is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation.

An example of an ISAO is the National Health Information Sharing & Analysis Center (NH-ISAC)

DHS: [http://www.dhs.gov/isao](http://www.dhs.gov/isao)

FDA’s Approach to Cybersecurity

Executive Orders
FDA Safety Communication
Draft Premarket Guidance
Begin Coordination with DHS
Recognize Standards
Establish Incident Response Team

2005: Issued guidance
2008: Halpern, et.al.
2009: Issued safety communication
2011: “Hacking” of implantable insulin pump (Radcliffe)
2012: First recall of vulnerable software (Roche - PC Anywhere)
2013: Recall of TNS-listener (Roche)

2014
Final Premarket Guidance
MOU with NH-ISAC
Public Workshop

2015
Draft and Final Postmarket Guidance
Public Workshop
MOU with NH-ISAC/MDISS

2016
Product-Specific Safety Comm
Build Ecosystem/Collaboration

2017
1st Cybersecurity WL

2018
Product-Specific Safety Comm
Questions?

Contacts:

CDRH mailbox, CyberMed@fda.hhs.gov
Seth Carmody, Seth.Carmody@fda.hhs.gov
Suzanne Schwartz, Suzanne.Schwartz@fda.hhs.gov