MEDICAL DEVICE CYBERSECURITY THROUGH THE FDA LENS

DITTA WORKSHOP ON CYBERSECURITY

19 MARCH 2018
SHANGHAI, CHINA

JEFF SHUREN, MD JD
CDRH CENTER DIRECTOR
US FDA

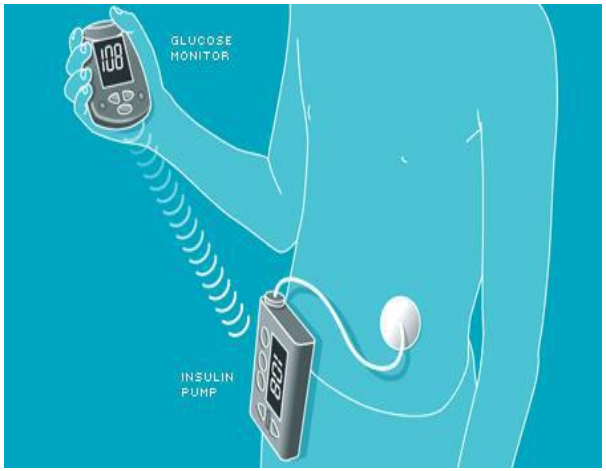
Bottom Line Up Front (BLUF)

- *"Whole of community"* approach: Collaboration is key
- Security spans across the total product lifecycle
- Impact on critical infrastructure within healthcare as well as across other sectors
- Integrate threat modeling from the early stages onward
- Foster culture and create incentives that encourage proactive behavior, *especially for information-sharing*

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

Medical Device Cybersecurity Background



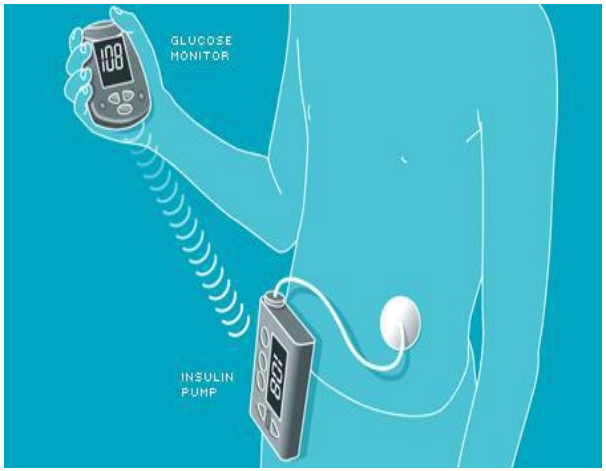
MEDICAL DEVICES

- Contain configurable embedded computer systems
- Increasingly interconnected
- Wirelessly connected
- Legacy devices

USE ENVIRONMENT

- Varied responsibilities for purchase, installation and maintenance of medical devices, often silo-ed
- Variable control over what is placed on the network
- Inconsistent training and education on security risks

Medical Device Vulnerabilities



- Network-connected medical devices infected or disabled by malware
- Malware on hospital computers, smartphones/tablets, and other wireless mobile devices used to access patient data, monitoring systems, and implanted patient devices
- Uncontrolled distribution of passwords
- Failure to provide timely security software updates and patches
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access

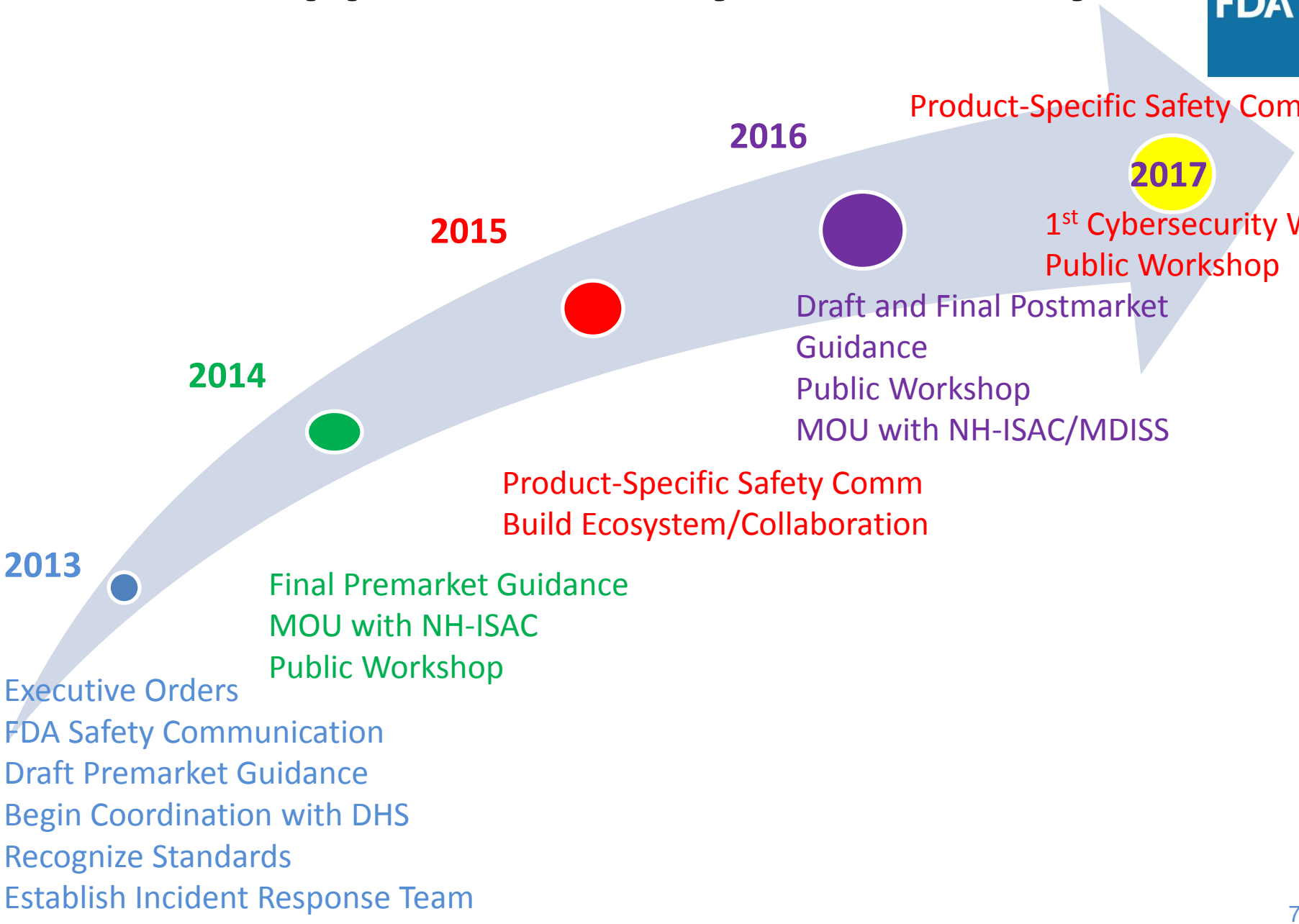
Executive Orders (EO), Presidential Policy Directives, and Framework to Strengthen Cybersecurity and Critical Infrastructure

- EO 13636 (Feb 2013)

"We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

- PPD 21 (Feb 2013)
- National Institute of Standards and Technology (NIST) Voluntary Framework (v1.0 - Feb 2014, v1.1 - draft Jan 2017)
- EO 13691 (Feb 2015) – establishment of Information Sharing and Analysis Organizations (ISAO)
- EO 13800 (May 2017) - "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

FDA's Approach to Cybersecurity



FDA Cybersecurity Work Products

U.S. Department of Health and Human Services

U.S. FOOD & DRUG ADMINISTRATION

A to Z Index | Follow FDA | En Español

Search FDA

Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices

Home > Medical Devices > Digital Health

Digital Health

- Cybersecurity
- Health IT Risk-Based Framework
- Medical Device Interoperability
- Mobile Medical Applications
- Wireless Medical Devices

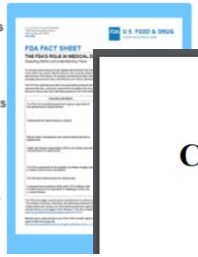
Cybersecurity

SHARE | TWEET | LINKEDIN | PIN IT | EMAIL | PRINT

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices.

All medical devices carry a certain amount of risk. The FDA allows devices to be marketed when there is a reasonable assurance that the benefits to patients outweigh the risks. While the increased use of wireless technology and software in medical devices also increases the risks of potential cybersecurity threats, these same features also improve health care and increase the ability of health care providers to treat patients.

Addressing cybersecurity threats, and thus reducing information security risks, is especially challenging. Because cybersecurity threats cannot be completely eliminated, manufacturers, hospitals and facilities must work to manage them. There is a need to balance protecting patient safety and promoting the



U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
FDA.GOV

U.S. FOOD & DRUG ADMINISTRATION

FDA FACT SHEET

THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

Dispelling Myths and Understanding Facts

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	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, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	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.
Medical device manufacturers can't update medical devices for cybersecurity.	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.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	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

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14,

For questions regarding this document contact the Office of Device Evaluation Office of Communication, Outreach and Development (CBER) at 1-800-835-4

Center for Devices and Radiological Health CDRH | CBER

Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

Premarket Cybersecurity Guidance

- Draft June 2013
- Final October 2014
- Key Principles:
  - 1) Shared responsibility between stakeholders, including healthcare 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 devices 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 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

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

Postmarket Cybersecurity Risk Assessment

Controlled Vulnerabilities

"Acceptable Residual Risk"

- Promote good cyber hygiene and reduce cybersecurity risks even when residual risk is acceptable
- Changes to a device solely to strengthen the cybersecurity associated with vulnerability with controlled risk are referred to as cybersecurity routine updates and patches and are typically considered to be device enhancements and are not required to be reported
- Annual reporting requirements for premarket approval (PMA) devices

Uncontrolled Vulnerabilities

"Unacceptable Residual Risk"

Guidance Addresses:

- Reporting Requirements
- Time Frame for Mitigating Risks
- Public Disclosure
- Information Sharing and Stakeholder Collaboration

Lessons Learned—Evolving Our Thinking

- Coordinated vs. non-coordinated disclosure of device vulnerabilities
  - Coordinated disclosure results in ability to get to ground truth as fast as possible so that mitigations can be proactively communicated and executed in a timely manner
  - Non-coordinated disclosure results in delayed assessments, communications, and mitigations
- Impact on HPH critical infrastructure and potential disruption of clinical care
  - Patching operating system is not yet routine with safety-critical systems
    - WannaCry Global Cyber Attack (May 2017)
    - Petya/notPetya (July 2017)
  - Delays in diagnosis/treatment intervention can result in patient harm too
- Potential for remote, multi-patient (i.e., scaled) attack of highest concern for harm

Key Takeaways

- *"Whole of community"* approach: Collaboration is key
- Security spans across the total product lifecycle
- Impact on critical infrastructure within and across sectors
- Integrate thread modeling from the early stages onward
- Foster culture and create incentives that encourage proactive behavior, *especially for information-sharing*