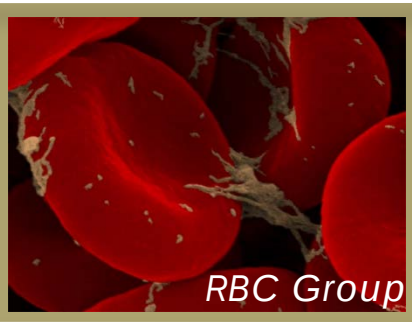
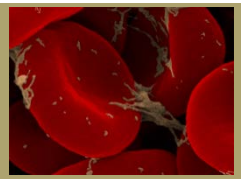
AMDM - Practical application of the FDA's Cybersecurity Guidance



John Roche

5 October 2017

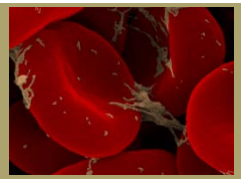
Personal Background



John Roche:

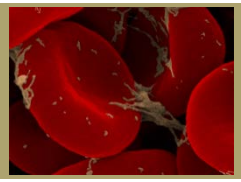
- Medical Diagnostics / Medical Device industry consultant since 2005 (RBC Group), focusing on product development, quality assurance and regulatory affairs
- Prior industry experience with Bayer Diagnostics, Abbott Laboratories and IDEXX Laboratories
- Educational Background in Biomedical Engineering, Electrical Engineering and Software Engineering

Agenda



- Practical application of the FDA's Cybersecurity Guidance
  - FDA Goals with New Guidance
  - Resources – FDA Website Cybersecurity Page
  - Progression of Cybersecurity
    - Premarket Cybersecurity Guidance (Oct '14)
    - Post Market Management of Cybersecurity in Medical Devices (Dec '16)
    - Other Recent Related Guidance
    - FDA Relationship to Other Groups
  - Recent Cybersecurity Related Recall
  - Cybersecurity – Myth vs. Facts (FDA Perspective)
  - General Applications – Corporate Level
  - Premarket Applications - Development
  - Postmarket Applications – Surveillance
  - Questions
  - References

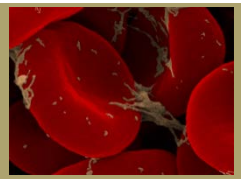
FDA Goals with New Guidance



- FDA desires manufactures to Implement a proactive, comprehensive risk management program:
  - Apply the National Institute of Standards and Technology (NIST) Framework to Strengthen Critical Infrastructure Cybersecurity
  - Establish and communicate processes for vulnerability intake and handling
  - Adopt a coordinated disclosure policy and practice
  - Deploy mitigations that address cybersecurity risk early and prior to exploitation
- Engage in collaborative information sharing for cyber vulnerabilities and threats

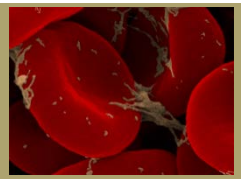
From FDA/CDRH Webinar 12 January 2017

Resources

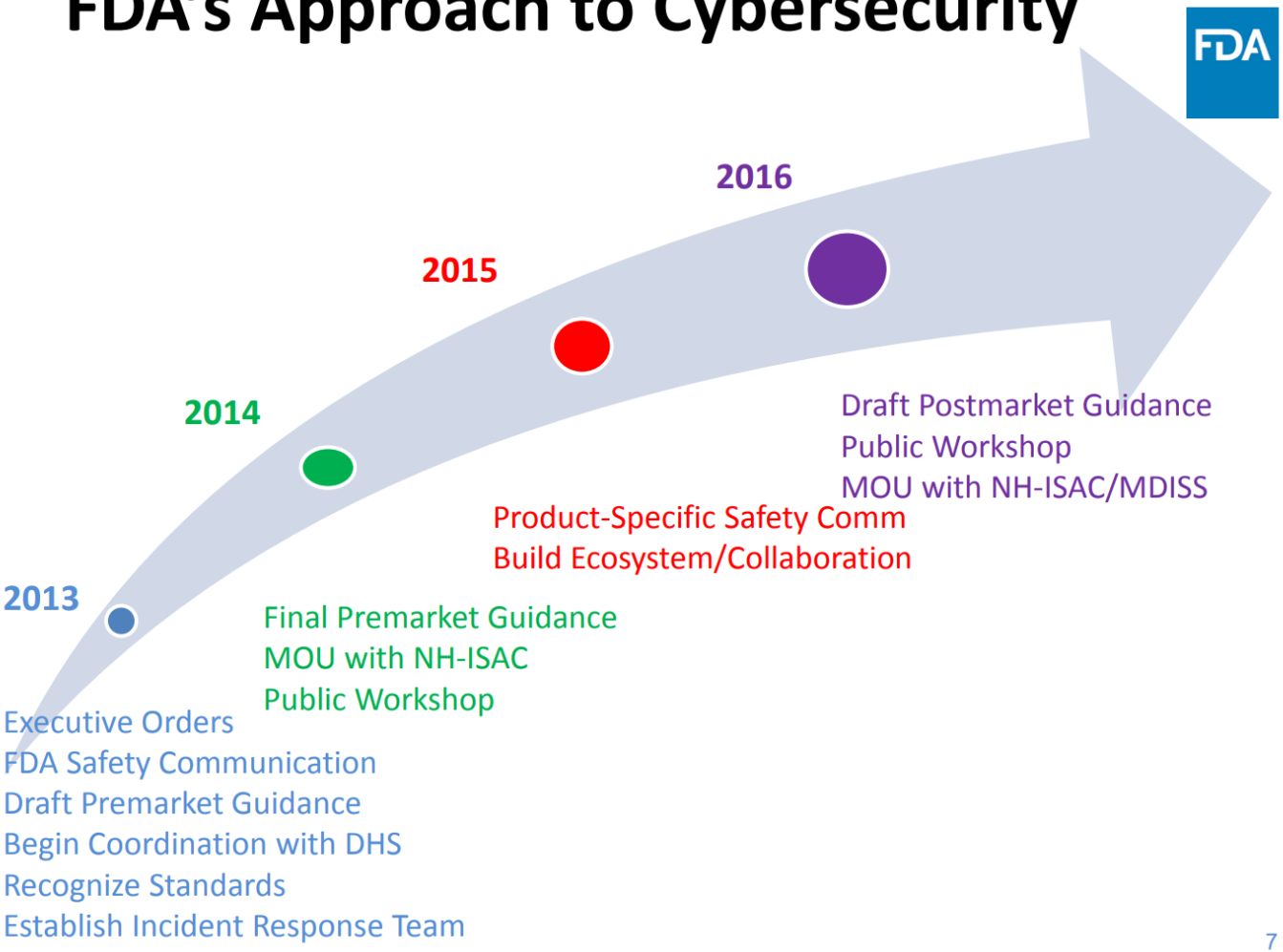


- FDA Website – Cybersecurity Page
  - https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213

Progression of Cybersecurity



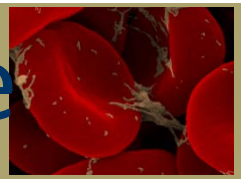
FDA's Approach to Cybersecurity



7

From FDA/CDRH Webinar 12 January 2017

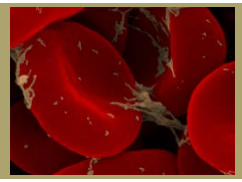
Premarket Cybersecurity Guidance



- Draft June 2013 / Final October 2014
  - 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)

From FDA/CDRH Webinar 12 January 2017

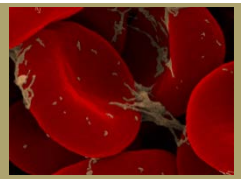
Postmarket Management of Cybersecurity



- Draft January 2016 / Final December 2016
  - 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

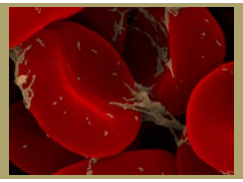
From FDA/CDRH Webinar 12 January 2017

Other Recent Related Guidance



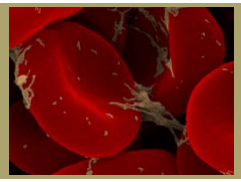
- Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices (Draft January ‘16 / Final Sept ’17)
  - Interoperable medical devices are devices as defined in section 201(h) of the (FD&C Act) that have the ability to exchange and use information through an electronic interface with another medical/nonmedical product, system, or device.
  - Interoperable medical devices can be involved in simple unidirectional transmission of data to another device or product or in more complex interactions, such as exerting command and control over one or more medical devices.
  - Interoperable medical devices can also be part of a complex system containing multiple medical devices

FDA Relationship to Other Groups



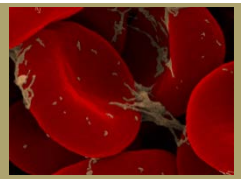
- In October 2016, the FDA entered into a new Memorandum of Understanding (MOU) with the National Health Information Sharing and Analysis Center (NH-ISAC) and the Medical Device Innovation, Safety and Security Consortium (MDISS).
- The NH-ISAC is a nonprofit health sector-led organization that provides member organizations with actionable information on cybersecurity and coordinates cybersecurity incidence response.

Myths vs Facts (FDA perspective)



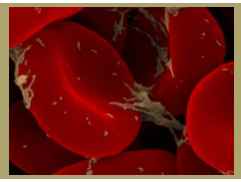
Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical 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 guidance's 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.

Myths vs Facts (FDA perspective)



Dispelling the Myths	Understanding the Facts
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 that are necessary.
The FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.	The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.
Companies that manufacture off-the-shelf (OTS) software used in medical devices are responsible for validating its secure use in medical devices.	The medical device manufacturer chooses to use OTS software, thus bearing responsibility for the security as well as the safe and effective performance of the medical device.

Recent Reported Cybersecurity Issue



FDA U.S. FOOD & DRUG ADMINISTRATION

Search FDA

Home > Medical Devices > Medical Device Safety > Safety Communications

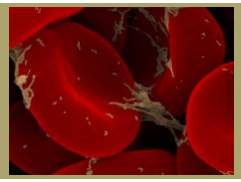
Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

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

Date Issued:

January 9, 2017

Recent Cybersecurity Recall



FDA U.S. FOOD & DRUG ADMINISTRATION

Search FDA

Home › Medical Devices › Medical Device Safety › Safety Communications

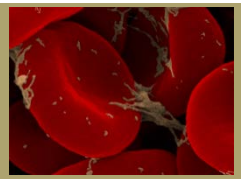
Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

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

Date Issued

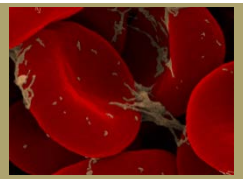
August 29, 2017

General Application – Corporate Level



- Establish Corporate Policies on Cybersecurity
  - Create a response plan with specific roles and responsibilities of key employees
  - Create a recovery plan specific roles and responsibilities of key employees
- Establish Procedures on Cybersecurity
- Establish Appropriate Training on Cybersecurity
- Establish Risk Assessment criteria for impact levels

General Application – Corporate Level

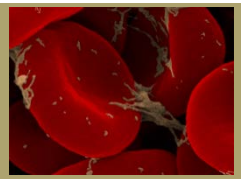


- From “Framework for Improving Critical Infrastructure”, NIST, February ‘14

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

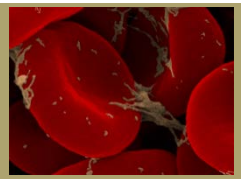
Figure 1: Framework Core Structure

Premarket Application - Development



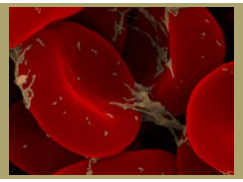
- Design Considerations
  - Security and Risk Management
  - Verification and Validation
  - Labeling
- Content of Premarket Submissions
  - Device Description
  - Risk Analysis
  - Verification and Validation
  - Labeling

Premarket Application - Development



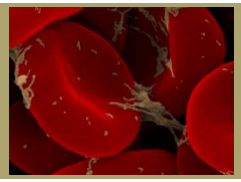
- Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis:
    - Identification of assets, threats, and vulnerabilities;
    - Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
    - Assessment of the likelihood of a threat and of a vulnerability being exploited;
    - Determination of risk levels and suitable mitigation strategies;
    - Assessment of residual risk and risk acceptance criteria.

Postmarket Application



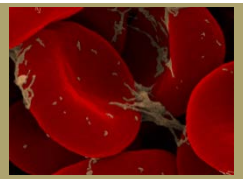
- Utilize Existing Mechanism of Quality System Regulation (21 CFR part 820)
  - Complaint Handling (21 CFR 820.198)
  - Quality Audit (21 CFR 820.22),
  - Corrective & Preventive action (21 CFR 820.100),
  - Software validation and Risk Analysis (21 CFR 820.30(g))
  - Servicing (21 CFR 820.200).

Postmarket Application

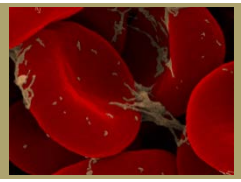


- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Maintaining software lifecycle processes that include evaluating Off The Shelf (OTS) software patches and updates related to vulnerability remediation.
- Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk;

Post Market – Risk Management



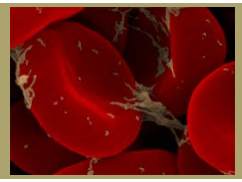
Post Market - Risk Management



- Controlled Risk - when there is sufficiently low (acceptable) residual risk of patient harm due to the vulnerability.

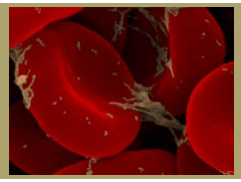
- Uncontrolled Risk: when there is unacceptable residual risk of patient harm due to insufficient risk mitigations and compensating controls.

Postmarket Application - Surveillance



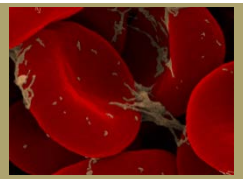
- The FDA's guidance to help reduce the impact of cybersecurity exploitation under a new initiative, is to have companies share their cybersecurity problems
- Companies voluntary participation in the 'Information Sharing Analysis Organizations' (IASOs)
- The IASOs functions as a cybersecurity information sharing and collaboration forum for the industry and the government

Postmarket Application - Surveillance



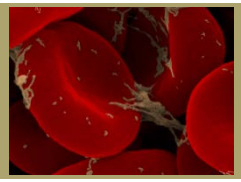
- Considerations if you opt for IASO:
  - What threat information may be shared?
  - What circumstances is it sharing appropriate?
  - Do items need to be redacted?
  - Are there other considerations to the business (legal, regulatory, corporate structure, etc.)

References



- Post Market Management of Cybersecurity in Medical Devices
  - https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
- FDA Fact Sheet on Cybersecurity
  - https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf
- Webinar - Postmarket Management of Cybersecurity in Medical Devices Final Guidance - January 12, 2017
  - https://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm534592.htm
- Cybersecurity for Networked Medical Devices containing OTS SW
  - https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf

References



- ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes;