Medical Device Cybersecurity: FDA Perspective

Suzanne B. Schwartz MD, MBA
Associate Director for Science and Strategic Partnerships
Office of the Center Director (OCD)
Center for Devices and Radiological Health (CDRH)
Food and Drug Administration (FDA)

FDA
C·D·R·H
Center for Devices and Radiological Health

Agenda

- Framing The Issue for Healthcare Public Health
- Timeline of FDA Activities
- Key Principles of Cybersecurity Premarket Guidance (FINAL issued Oct 2014)
- Key Principles of Postmarket Management of Cybersecurity in Medical Devices (DRAFT guidance January 2016)
- Summary & Next Steps

FRAMING THE ISSUE: ENVIRONMENT

- The health care and public health (HPH) sector represents a significant and large attack surface
  - Intrusions and breaches occur through weaknesses in the system architecture
- Connected medical devices, like all other computer systems, are vulnerable to threats
- 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
  - May serve as a safety issue

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

- EO 13636 (Feb 2013) - Improving Critical Infrastructure Cybersecurity
- PPD 21 (Feb 2013) - Critical Infrastructure Security and Resilience
- NIST Voluntary Framework (Feb 2014)
- EO 13691 (Feb 2015) – Promoting Private Sector Cybersecurity Information Sharing

Timeline of Key FDA Activities

- **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

    http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
  - 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

    (http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf)

Key Activities intended to:

- Inform key concepts of FDA's current thinking with respect to premarket and post market management of medical device cybersecurity:
  - 'Essential clinical performance' and potential impact on patient safety
  - Integration of threat modeling
  - Information-sharing and timely remediation
- Discuss stakeholders' interpretation and identify implementation challenges
- Obtain input from healthcare and public health sector stakeholders on information sharing needs

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)

Premarket Cybersecurity Submission Expectations

- Risk Management (threat modeling)
  - Inclusion of hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device, including:
    - A specific list of all cybersecurity risks that were considered in the design of your device;
    - A specific list and justification for all cybersecurity controls that were established for your device.
- Traceability
  - Inclusion of a traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered

Premarket Cybersecurity Submission Expectations

- Lifecycle Plans
  - Plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device
  - A summary describing controls that are in place to assure that the medical device software will maintain its integrity (e.g. remain free of malware) from the point of origin to the point at which that device leaves the control of the manufacturer
- Labeling
  - Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g. anti-virus software, use of firewall)

Key Principles of Postmarket Management of Cybersecurity in Medical Devices

- 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

Use of NIST Framework

- Both Guidance documents recommend use of NIST Cybersecurity Framework's 5 core functions
  - Identify
  - Protect and Detect
    - Vulnerability assessment and risk analysis
  - Respond and Recover
    - Compensating controls, risk mitigation and remediation

Postmarket Cybersecurity Guidance - DRAFT

Cybersecurity risk management programs should include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risk early and prior to exploitation

Information Sharing and Analysis Organizations (ISAO)

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;

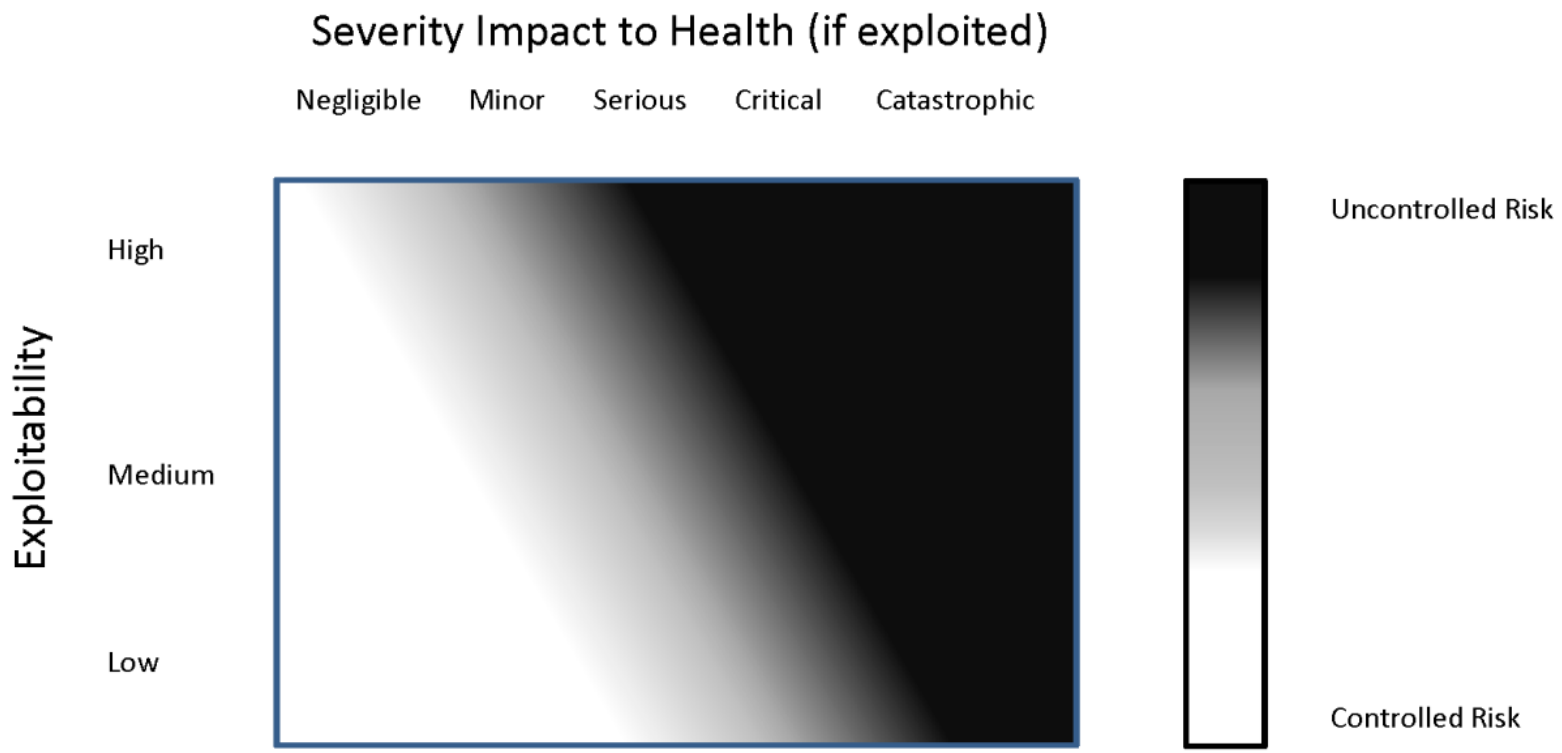
Actionable - groups will receive useful and practical cybersecurity risk, threat indicator, and incident information via automated, real-time mechanisms if they choose to participate in an ISAO;

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.

See: http://www.dhs.gov/isao

Medical Device Cybersecurity Risk Management



Summary and Next Steps

- Medical device cybersecurity requires a total product life cycle approach: from design to obsolescence
- FDA's proposed regulatory policy incentivizes proactive behavior and good cyber hygiene
- Strengthening cybersecurity within the healthcare and public health sector is a collective effort amongst all stakeholders
- Development and validation of meaningful tools for assessment of vulnerabilities in the clinical environment is an area of focus going forward

FDA Resources

- FDA Medical Device Cybersecurity Webpage:
  - http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

- Postmarket management of cybersecurity in medical devices – DRAFT Guidance:
  - http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf