THE EVOLVING MEDICAL DEVICE CYBERSECURITY ECOSYSTEM

SUZANNE B SCHWARTZ, MD, MBA

CDRH / FDA

SOFTWARE & SUPPLY CHAIN ASSURANCE FORUM

MITRE, MCLEAN CAMPUS

DECEMBER 19, 2018

Lessons Learned—Evolving Our Thinking

- Coordinated vs. non-coordinated disclosure of device vulnerabilities
  - Ability to get to ground truth as fast as possible so that mitigations can be proactively communicated and executed in a timely manner
    - JnJ Animas Insulin Pump
  - Non-coordinated disclosure results in delayed assessments, communications, and mitigations
    - St Jude/Abbott pacemakers and ICDs
- Impact on HPH critical infrastructure and potential disruption of clinical care
  - Patching operating system is not 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

Medical Device Safety Action Plan:
Advancing Medical Device Cybersecurity

- Update 2014 premarket guidance
- Consider seeking additional premarket and postmarket authorities to:
  - Require that firms build capabilities to update and patch device security into a product's design and to include appropriate data supporting this capability in premarket submissions to FDA for review
  - Require firms to develop a "Software Bill of Materials" (SBOM) and to share with customers
  - Require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified
- Request appropriations for seeding establishment of a CyberMed Safety (Expert) Analysis Board (CYMSAB) functioning as a public-private model, and serving the ecosystem as a neutral entity

2018 Reflections

- Medical Device Safety Action Plan (April 2018)
- Perspective piece in American Heart Association Journal 'Circulation' (Sept 2018)
- Report on Advancing Coordinated Vulnerability Disclosure – MDIC publication (Oct 2018)
- FDA Commissioner's Statement (Oct 2018):
  - Strong commitment to efforts that bolster medical device cybersecurity
  - Regional Incident Preparedness & Response Playbook – MITRE publication (Oct 2018)
  - Execution of 3-way MOUs with H-ISAC for 2 newly stood up ISAOs for medical device vulnerability reporting (Oct 2018):
    - MedISAO
    - Sensato

2018 Reflections continued

- New FDA Draft Premarket Cybersecurity Guidance & Announcement of FDA convened Public Workshop, Jan 29-30, 2019
- Execution of MOA with Department of Homeland Security

2018 Premarket Draft Guidance: Revision Background

- New guidance is needed as medical device cybersecurity continues to evolve
- Changes proposed to the guidance based on lessons learned from routine vulnerability management, response activities, engaging stakeholders including working with manufacturers pre- and post-market.
- Examples of recent threats:
  - Malware/ransomware attacks, e.g., WannaCry, notPetya, Meltdown and Spectre

Revision Approach

- Leveraged the 2014 premarket guidance document
  - Kept alignment with NIST 5 core functions
  - Similar structure
  - Maintained focus on documentation related to requirements of the QSR (21 CFR Part 820)

- Provided additional granularity to help manufacturers implement cybersecurity in the premarket setting
  - Expanded on maintaining properties of authenticity, availability, integrity, and confidentiality through design, risk management, and labeling
  - Labeling grounded in statutory and regulatory requirements; for example:
    - Adequate directions for use, 21 CFR 801.5
    - For prescription devices, 21 CFR 801.109(c)

What's New

- Designing trustworthy devices
- Preventing multi-patient attacks
- Tiering system – information to be provided in premarket submission is geared to level of risk:
  - Tier 1 – higher risk
  - Tier 2 – lower risk
- Cybersecurity Bill of Materials
  - Leverages purchasing controls in QSR (21 CFR 820.50)
- System level threat models

Looking Ahead 2019

- Complete CVSS clinical rubric & submit for MDDT qualification (MITRE-led WG)
- Further enhance public-private partnership collaborations to collectively address Imperative 2 of 2017 Task Force Report:
  - HSCC Task Group 1B *soon to be released* Joint Security Plan
  - CYMSAB Pilot currently under development (with MITRE support)
  - Additional ISAOs in formation for device vulnerability info-sharing
  - Dedicated effort on defining and operationalizing Software Bill of Materials

Looking Ahead 2019 continued

- International Medical Device Regulators Forum (IMDRF) new medical device cybersecurity work item:
  - FDA and Health Canada co-leads
- Expand x-stakeholder participation in DefCon Biohacking Village Device Hacking Lab, with the following goals:
  - Increase medical device manufacturer (MDM) presence
  - Introduce to clinical community
  - Engage HDOs
- Leverage cross-agency / multi-stakeholder collaborative efforts:
  - NTIA (Dept of Commerce) Multi-stakeholder engagement on software component transparency includes representation on WGs from: HDOs, MDMs, device trade organizations and FDA
  - NCCoE (NIST/Dept of Commerce) working with industry to develop use cases for medical device security

Medical device cybersecurity is a shared responsibility

Your input is important to us!

FDA contacts:

Suzanne.Schwartz@fda.hhs.gov
Seth.Carmody@fda.hhs.gov
Aftin.Ross@fda.hhs.gov

Or email the team:

CyberMed@fda.hhs.gov

https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm