Medical Device Cybersecurity: FDA & the Community

CyberMedRx Summit
Microsoft Tech Center
Cambridge, MA
Friday December 4th, 2015

Suzanne B. Schwartz, MD, MBA
Associate Director for Science & Strategic Partnerships
Director (Acting) Emergency Preparedness/ Operations & Medical Countermeasures (EMCM)
Office of the Center Director
CDRH/FDA

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

FACTS:

- **Our Mission**: safe and effective medical devices
- **Our Statutory Authority**: Federal FD & C Act
- **Our Goals:**
  - Raise cyber-security awareness
  - Leverage knowledge from other industry sectors
  - Promote safety and security by design by clear regulatory expectation
  - Promote coordinated vulnerability disclosure & proactive vulnerability management
  - Minimize reactive approaches
  - Foster ***'whole of community'***

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

FACTS:

- ***FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity***
- ***FDA has highlighted Medical Device Cybersecurity within the top ten FY 2016 Regulatory Science Priorities:***
  - http://www.fda.gov/MedicalDevices/ScienceandResearch/ucm467550.htm
- ***FDA is shifting the paradigm: will not wait for adverse events to occur in order to spur action.***
- ***FDA is working with all of our stakeholders to change the culture of engagement***

CDRH/FDA Collaborations & Key Engagements

- Partnering with **Department of Homeland Security**
  - Coordinating vulnerability assessment and incident response with ICS-CERT
  - Jointly participating in outreach opportunities (conference panels)
- Enhanced communication & partnering with other **HHS OPDivs**
  - ASPR Critical Infrastructure Protection
  - ONC
  - OCR
  - OCIO
  - OSSI
- Strengthen collaboration with **NIST**
  - through standards efforts, NCCoE infusion pump use case
- Engaging proactively with **Diverse Stakeholders in Private Sector**
  - Outreach to HDOs, end users, medical device supply chain, & security researcher community
- MOU with **NH-ISAC**
- **NH-ISAC** and **MDISS** collaboration
- **DTSec Project** – public-private initiative developing security standards for diabetes devices
- Contract with **MITRE**

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

What's Next? Address Current Gaps via:

- **Articulating Expectations for Postmarket Management** of Medical Device Cybersecurity
  - Total Product Lifecycle Approach for Safety and Security!!
- **Adapting the NIST Framework** for the Medical Device Ecosystem
- **Translating the Common Vulnerability Scoring System** for medical devices and the clinical use environment
- **Promoting adoption of vulnerability disclosure policy** with coordinated vulnerability disclosure & proactive vulnerability management

Principles & Opportunities for Greater Impact

Key Principles:

Cybersecurity of Medical Devices is a total product lifecycle approach, from design to obsolescence.

Vulnerability disclosure policy, coordinated disclosure and proactive vulnerability management are critical to improving the security posture and SAFETY of the medical device ecosystem as a whole.

What We Need:

- For all stakeholders to recognize their role
- To change the culture of engagement
- To make cyber hygiene paramount
- To create a trusted environment for information sharing
- The right tools which can serve as enablers for VULN assessment, disclosure and remediation

SAVE THE DATE: January 20th and 21st, 2016

2nd FDA Medical Device Cybersecurity Public Workshop

http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm474752.htm

PLEASE JOIN US!!!

"Safeguarding our Patients: Harnessing the Collective Will & Creating a Culture of Multi-Stakeholder Collaboration for Medical Device Security"

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