# Medical Device Cybersecurity: Moving The Needle Together

8th Annual Safeguarding Health Information:
Building Assurance through HIPAA Security
HHS Office of Civil Rights and
National Institute of Standards & Technology
Wednesday September 2, 2015

FDA

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

**Suzanne B. Schwartz, MD, MBA**
**Director Emergency Preparedness/Operations & Medical Countermeasures (EMCM Program)**
**CDRH/FDA**

*"Imagination will often carry us to worlds that never were. But without it we go nowhere."*

*- Carl Sagan*

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


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

# *September is National Preparedness Month*

***"Failing to prepare***

***means preparing to fail"***

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

# *Three Core Concepts*

- Awareness
- Preparedness
- Collaboration

# *Why does FDA care about Cybersecurity?*

- Networked medical devices facilitate care
- Networked medical devices introduce new risks

- Centers for Disease Control and Prevention (CDC) estimates of annual patient encounters
  - 35 million hospital discharges
  - 100 million hospital outpatient visits
  - 900 million physician office visits
  - Billions of prescriptions
- Most of these encounters likely include a networked medical device

# *Also the President said so…*

**Presidential Policy Directive 8 (PPD-8):** National Preparedness Post-Katrina: "federal departments and agencies to work with the whole community to develop a national preparedness goal and a series of frameworks and plans related to reaching specified goals."

**PPD-21:** Critical Infrastructure Security and Resilience

**Executive Order 13636:** Improving Critical Infrastructure Cybersecurity a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure

**Executive Order 13691:** Promoting Private Sector Cybersecurity Information Sharing (2/13/2015)

https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

| | | | |
|---|---|---|---|
| Chemical | Commercial Facilities | Communications | Critical Manufacturing |
| Dams | Defense Industrial Base | Emergency Services | Energy |
| Financial Services | Food and Agriculture | Gov't Facilities | Healthcare and Public Health |
| IT | Nuclear | Transportation | Water/Wastewater |

# *CDRH/FDA Goals*

- Meet our mission: safe and effective devices
- 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'*** approach


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

# *Today's Key Takeaways*

- FDA seeks to foster a 'whole of community' approach
- Establish a Cybersecurity Risk Management Program
- Make cyber hygiene paramount
- Create a trusted environment for information sharing
- Software updates for cybersecurity do not require pre-market review or recall (there are some exceptions)
- FDA will not be prescriptive with risk analyses
- Vulnerability disclosure policy and coordinated disclosure are critical to improving the security posture of the ecosystem as a whole

# *Roadmap for Today's Discussion*

- The Year in Reflection
- CDRH/FDA Medical Device Cybersecurity Current Efforts
- Our Vision Ahead

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

# ECOSYSTEM

Uncertainty

Competing Needs

Complex


Evolving

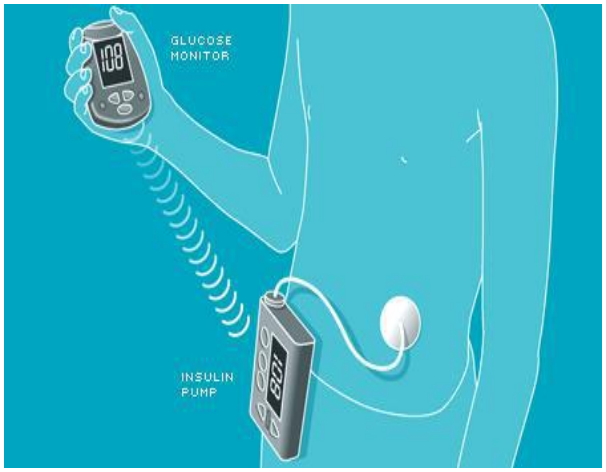
Diverse

Enormous

Interconnectedness

Lagging

# *Incidents & Researcher-Demonstrated Exploits*




- VA Cath Lab temporary closure (1/10) due to malware infecting computers used during interventional cardiac procedures
- “Hacking” of implantable insulin pump (Radcliffe, 8/11)
- Security researchers present CDRH with cyber vulnerabilities of medical devices due to hardcoded passwords (Rios & McCorkle, 4/13)
- Vulnerabilities identified in PCA and other Infusion Pumps (Rios, 5/14-6/15)

# *CDRH/FDA Activities*

- **Guidance**
  - Premarket (Final 2014)
  - Wireless Technology (2013)
  - CS for Networked Devices with OTS Software (2005)
- **Standards**
  - Cybersecurity (2013)
  - Interoperability (2013)
- **Public Communication**
  - Safety Communication to Stakeholders (June 2013, May 2015 and July 2015)
  - CS for networked medical devices shared responsibility (2009)
- **Organization**
  - Established CSWG of Subject Matter Experts (2013)
  - Stood up Cyber Incident Response Team under EMCM (2013)

# *CDRH/FDA Collaborations*

- 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 **HHS**
  - Critical Infrastructure Protection, CTAC
  - ONC, OCR
- Strengthen collaboration with **NIST**
  - through standards, CSF Working Group, infusion pump use case
- Engaging proactively with **Diverse Stakeholders**
  - Outreach to hospital, healthcare, medical device & information security researcher community
- MOU with **NH-ISAC**
- **NH-ISAC** and **MDISS** collaboration
- **DTSec Project** - developing security standards for diabetes devices

# *CDRH/FDA and MITRE*

Advance the CDRH Medical Device Security Vision via -

- Stakeholder Engagement
- Develop Vulnerability Ecosystem Roadmap
- Analyze and design a “trusted environment” for collecting, analyzing, and sharing (possibly sensitive) medical device vulnerability and security information.

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

# *FDA Public Workshop: 'Collaborative Approaches for Medical Device and Healthcare Cybersecurity'*

- **October 21-22 2014**
- **Co-sponsored with HHS and DHS**
- **1300 total participants included onsite and remote**
  - Broad range of stakeholders
- **Goals:**
  - **Catalyze collaboration among all HPH stakeholders**
  - **Identify barriers that impede efforts towards promoting cybersecurity**
  - **Advance the discussion on innovative approaches for building securable medical devices**

# *FDA Public Workshop* *continued*

## *Focus Areas:*

- Increasing awareness
- Understanding cybersecurity gaps and challenges
  - Legacy devices
- Exploring tools and standards
- Leveraging expertise
- Establishing a collaborative model for information sharing and a shared risk-assessment framework

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

# *Systemic Challenges*

- Growing cyber threat
- Cybersecurity may not be on the radar of the C-suite
- No safe space for information-sharing
- Lack of a common lexicon
- Lack of standards for device integration and maintenance
- No one-size fits all solution
- Cybersecurity isn't just a design issue; it's a lifecycle issue
- Incomplete rules of engagement

# *Stakeholder Challenges*

- Lack of trust
- Many stakeholders addressing cybersecurity in silos
    - Some may not understand the clinical environment
- Cyber-researchers bring disruption to the community
- A lot of smaller organizations without the cybersecurity resources or expertise

# *Stakeholder Challenges continued*

- Stakeholders don't know how to prioritize vulnerabilities
- Stakeholders may not know all of the standards and tools that exist and which are best
- *What is the value proposition?*

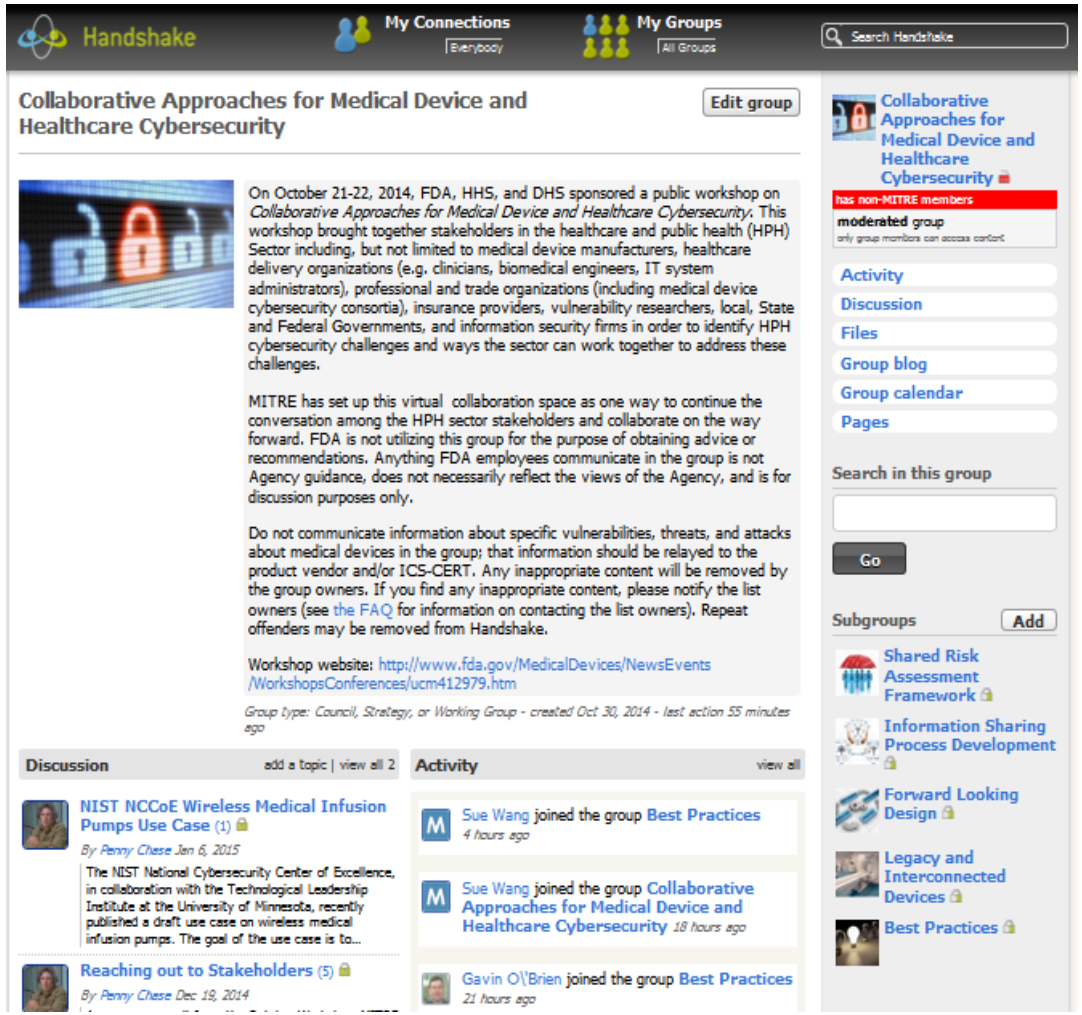
# *Handshake Virtual Collaboration Tool*

## Goal:

- Keep promise made at public workshop to provide a virtual space to continue the conversation
- MITRE hosts a business networking site to support relationships and collaboration among MITRE, government sponsors, industry, and academia

# Handshake Site – hosted by MITRE
# Medical Device & Healthcare Cybersecurity

- Created site
  - Top-level group and sub-groups
  - Initial content
- Drafted a FAQ with “rules of engagement”
- Sent invitation email to the 1300 workshop participants on December 18
  - Individual requests account
  - MITRE sends invitation
  - Individual responds and creates account
  - Individual joins Handshake



# *A Few Words about FDA's Premarket Guidance…. (Final Published on 10/2/2014)*

- Shared responsibility between stakeholders
- Address during design and development
  - 'Baked in not bolted on'
  - Secure design starts with a good process
- Cybersecurity vulnerability and management approach established as part of software validation and risk analysis as required by 21 CFR 820.30(g)
- Alignment with NIST Cybersecurity Framework 5 core functions: *identify, protect, detect, respond and recover*
- ***FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity***

# *Cybersecurity Risk Management Program*
# *Step 1:* Adopt a Cybersecurity Culture

- Premarket
  - 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.
- Post Market
  - Engage in post market surveillance and Information Sharing and Analysis Organizations (ISAOs)
  - Assess the device impact and clinical impact of vulnerabilities and exploits
  - Address the risk; actions taken should be commensurate with the risk
  - Disseminate, Incorporate and Iterate

# *Cybersecurity Risk Management Program*
# *Step 2:* Produce Objective Evidence

- **Premarket**
  - Device design features that mitigate cybersecurity risk
  - Subset of software documentation (Premarket Submissions for Software contained in medical devices
    - Software description, **hazards**, **requirements**, design spec, **traceability**, development environment, **Verification and Validation**, revision history, and **unresolved anomalies** (vulnerabilities?)

- **Post Market**
  - Produce objective evidence that could include policies, procedures, CAPAs, complaints, information sharing, etc.

# *What documentation is FDA looking for?*

- **Hazard Analyses**
  - **Evaluate both intentional and unintentional cybersecurity risk**
    - Provide information on the risk analyzed
  - **Controls established to mitigate risk**
    - Provide information on the controls put in place
    - Provide information on the appropriateness of the controls to mitigate identified risk
  - **Matrix that links cybersecurity controls to the risk being mitigated**
  - **Summary documentation on**
    - Plan to provide validated patches / updates
    - Plan to assure device integrity
  - **Cybersecurity control instructions pertaining to use environment**
  - **A systematic plan for providing patches and updates to operating systems or medical device software.**

# *Best Practices and Tools*

- **Adopt a Cybersecurity Culture** (Start with NIST):
  - Robust Cybersecurity cultures exist across multiple economic sectors including the financial, utility, and defense sectors.
  - Risk mitigation during total product life cycle from conception to obsolescence
  - Information Sharing (with all stakeholders)
  - Identify, Protect, Detect, Response, Recover
  - Integrate and Iterate
  - Hire/contract with, appropriate personnel
  - Security first, implement design features as well as compensating controls
  - Cyber hygiene (configuration, access control, etc.)

http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm

http://www.counciloncybersecurity.org/critical-controls/

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

# *Campaign for Cyber Hygiene*

- ***Cyber hygiene*** is a state of diligent control of a device's operation, exercised in the use environment and considered ***'best practice'*** by the security community. This best practice is comprised of safe and proper configuration of available features, least privilege access to control functions and cybersecurity routine servicing. These practices are undertaken in order to maintain and improve cybersecurity. Additional cyber hygiene controls are identified by FDA in the cybersecurity premarket guidance.

http://www.counciloncybersecurity.org/critical-controls/

# *What's Next?*

- **Articulating Postmarket Expectations** for 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 (CVSS)** for medical devices and the clinical use environment
- **Promoting adoption of vulnerability disclosure policies** with coordinated vulnerability disclosure & proactive vulnerability management

# *In Summary - Today's Key Takeaways*

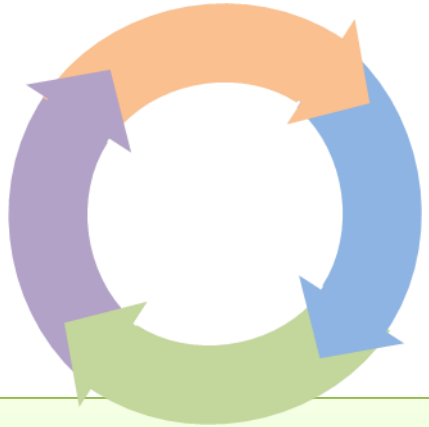
- Establish a Cybersecurity Risk Management Program
- Make cyber hygiene paramount
- Create a trusted environment for information sharing
- FDA seeks to foster a 'whole of community' approach
- Software updates for cybersecurity do not require pre-market review or recall (there are some exceptions)
- FDA will not be prescriptive with risk analyses
- Vulnerability disclosure policy and coordinated disclosure are critical to improving the security posture of the ecosystem as a whole

# CDRH/FDA Forward Looking Vision

*Post market surveillance*

*Regulatory clarity*

- *Premarket expectations*
- *Post market expectations*



*Stake holder collaboration*

- *Device industry*
- *Healthcare organization*
- *Federal partners*
- *Researchers & experts*

*Enable a platform for maintaining Cybersecurity Awareness –*

*Intentional and unintentional threats*

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

*"Logic will get you from A to B. Imagination will take you everywhere."*

*- Albert Einstein*

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

# THANK YOU!

# QUESTIONS?

Suzanne.Schwartz@fda.hhs.gov