Medical Device Cybersecurity and FDA

IVD Roundtable

Dharmesh Patel

June 2, 2016

For FDA, Cybersecurity is Key to Device Safety & Effectiveness

- Networked medical devices facilitate care, but also introduce new risks that can result in patient illness, injury, or death
  - Compromised device functionality
  - Loss of data availability or integrity
  - Exposure of other connected devices or networks to security threats
- CDC estimated approx. 51M procedures and 1.2B physician/hospital outpatient/ER visits in 2010*. Many of these encounters involved networked medical devices.

* http://www.cdc.gov/nchs/fastats/hospital.htm, http://www.cdc.gov/nchs/fastats/physician-visits.htm

Prepare for Cybersecurity Threats During Premarket Activities

- FDA Cybersecurity Guidance: Premarket Submissions (Oct 2014)
- Medical device security is a shared responsibility among stakeholders
- Manufacturers should address cybersecurity during design and development
  - Determine cybersecurity-related design inputs
  - Include a cybersecurity vulnerability and management approach in software validation and risk analyses
- Consider cybersecurity framework core functions
  - Identify, Protect, Detect, Respond, Recover

FDA Premarket Cybersecurity Guidance: Q&As

- Q: Is FDA premarket review required prior to implementation of a software patch to address a cybersecurity vulnerability?
  - A: "The FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity."

- Q: How should cybersecurity-related software updates and patches be documented?
  - A: Firms should include a summary describing the plan for providing validated software updates and patches throughout the lifecycle of the medical device to continue to assure safety and effectiveness.

Monitor and Address Cybersecurity Vulnerabilities Postmarket

- Postmarket Management of Cybersecurity In Medical Devices
  - ***Draft Guidance*** released January 2016
- Comprehensive Cybersecurity Risk Management:
  - Know
  - Assess
  - Fix

Draft Postmarket Guidance Does Not Propose a Change To Existing Policy

- **Existing Policy:** For cybersecurity routine updates and patches, the FDA will, typically, not need to conduct premarket review to clear or approve the medical device software changes

Because Risks Evolve, Can't Mitigate With Only Premarket Controls

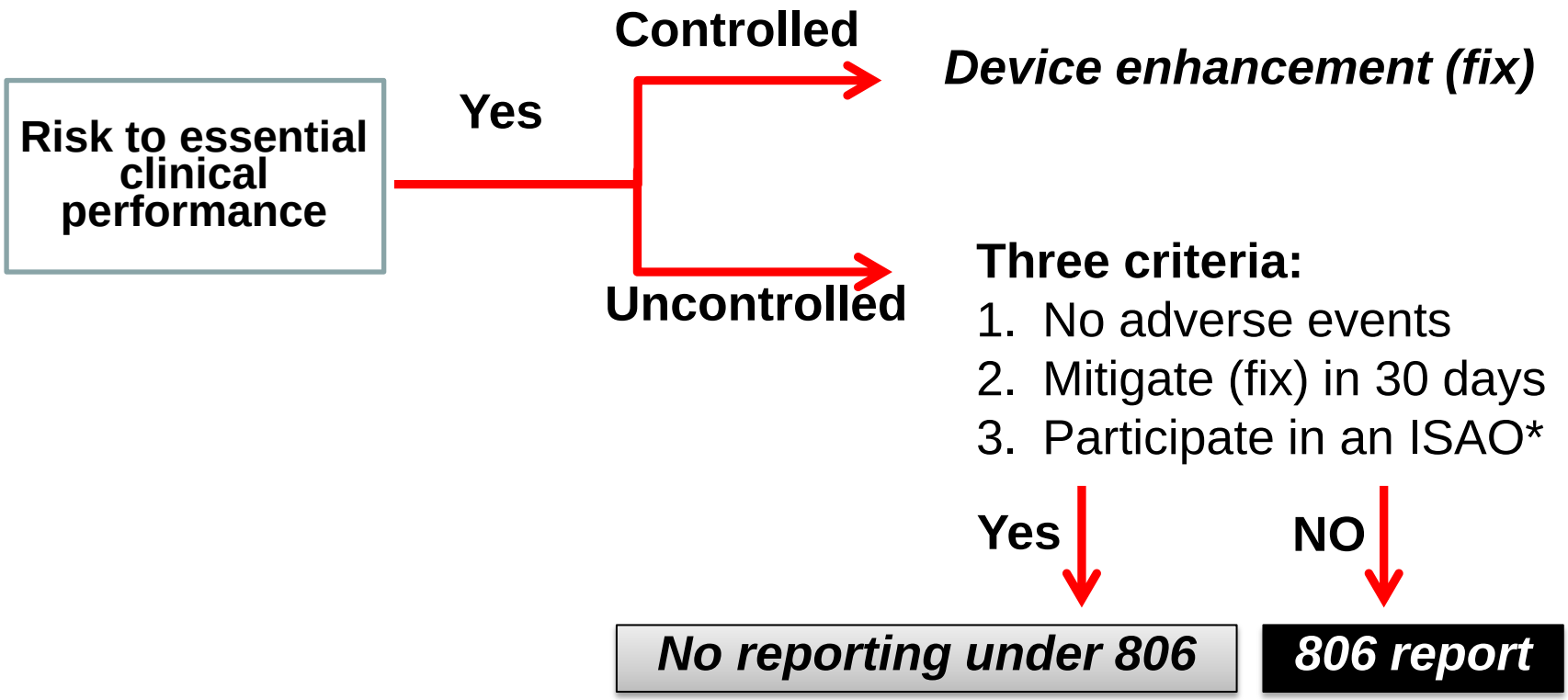
- Leverage existing Quality System Regulation
- Manufacturers should respond in a timely fashion to address identified vulnerabilities
  - Monitor Cybersecurity information sources
  - Understand, assess, and detect
  - Establish processes for vulnerability handling
  - Develop mitigations
  - Adopt a coordinated disclosure policy
  - Deploy mitigations early and prior to exploitation

When do I Assess?

Always

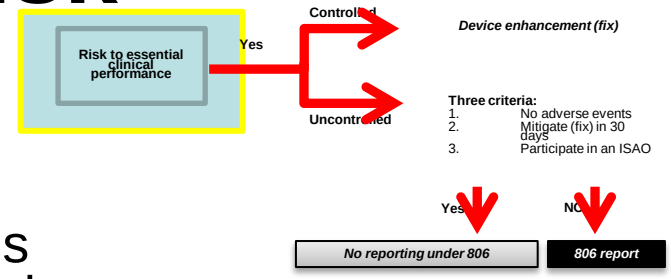
It is the vulnerability that matters

Reducing Risk is Essential

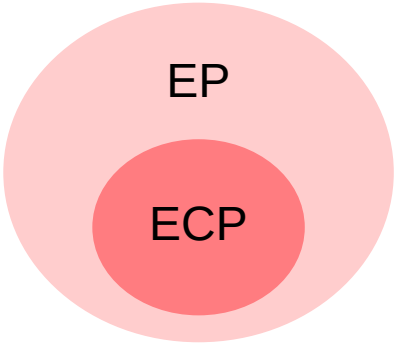


From "Postmarket Management of Cybersecurity in Medical Devices" DRAFT version January 22, 2016
*ISAO (Information Sharing and Analysis Organization)

Essential Clinical Performance = Freedom From Clinical Risk



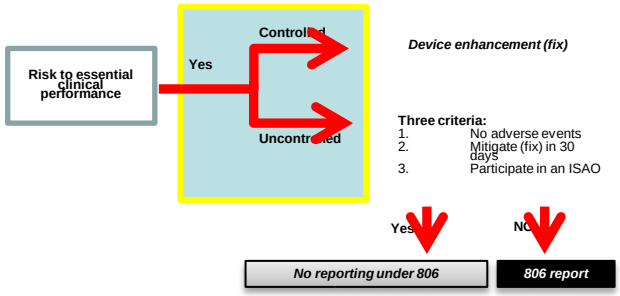
- **Essential clinical performance (ECP)** means performance that is necessary to achieve freedom from unacceptable clinical risk, as defined by the manufacturer.
- Compromise of the essential clinical performance can produce a hazardous situation that results in harm and/or may require intervention to prevent harm.
- A new concept, derived from IEC 60601* – Essential Performance (EP)
  - Performance necessary to achieve freedom from unacceptable risk



From "Postmarket Management of Cybersecurity in Medical Devices" DRAFT version January 22, 2016

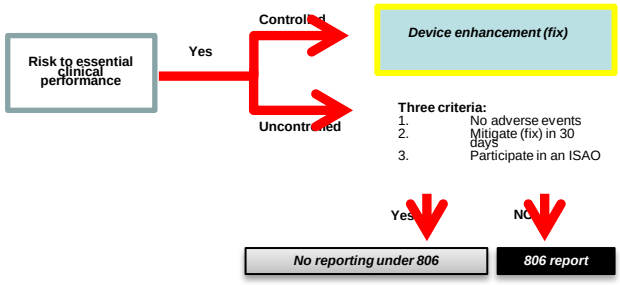
*IEC 60601-1:2005, *Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance*, Section 3.27

ECP Risk Evaluation Leads to a Binary Determination: Controlled vs Uncontrolled



From “Postmarket Management of Cybersecurity in Medical Devices” DRAFT version January 22, 2016

Controlled Risk = Acceptably Low Risk That ECP Could Be Compromised

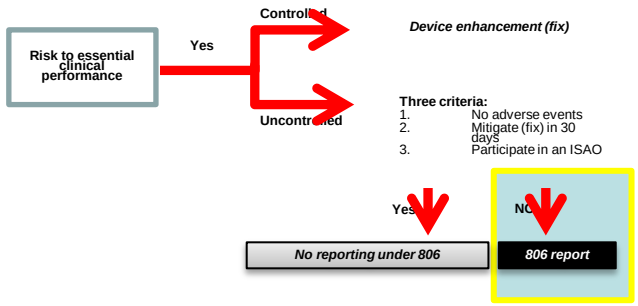


- Device Enhancements
- Changes to a device made solely to strengthen cybersecurity
  - Routine Updates, Patches

- For PMA devices, report in an periodic (annual) report

From “Postmarket Management of Cybersecurity in Medical Devices” DRAFT version January 22, 2016

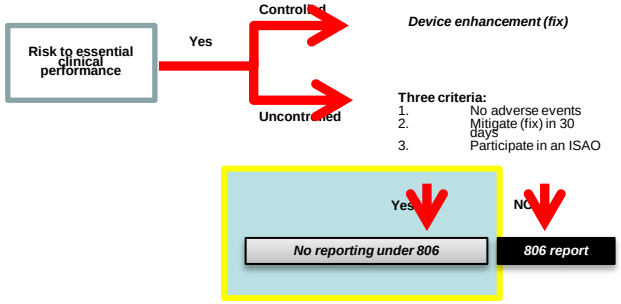
Uncontrolled Risk = Additional Risk Controls Needed



- Remediate vulnerabilities
- Identify and implement compensating controls
- Report vulnerabilities to FDA (21 CFR part 806)**
- Evaluate changes to assess need for a premarket submission
- In the absence of remediation, product may be considered in violation of FD&C Act and subject to action

From “Postmarket Management of Cybersecurity in Medical Devices” DRAFT version January 22, 2016

806 Reports are Not Always Necessary, Even When Initial Risk to ECP is Uncontrolled



- FDA does not intend to enforce reporting requirements under 21 CFR part 806 if all the following met:
  - No known adverse events or deaths
  - Fix within 30 days
  - Participate in an Information Sharing and Analysis Organization (ISAO), such as NH-ISAC

From “Postmarket Management of Cybersecurity in Medical Devices” DRAFT version January 22, 2016
For additional ISAO details see: http://www.dhs.gov/isao

CDRH/FDA Activities

- **Guidance**
  - Postmarket Cybersecurity (Draft Jan 2016)
  - MDDS (Medical Device Data Systems – Final 2015)
  - MMA (Mobile Medical Applications – Final 2015)
  - Premarket Cybersecurity (Final Oct 2014)
  - Wireless Technology (Final 2013)
  - Cybersecurity for Networked Devices with OTS Software (2005)
- **Recognized Standards**
  - Cybersecurity IEC 29147 (2013)
  - Interoperability (2013)
- **Public Communication**
  - Public Workshop – Moving Forward: Collaborative Approaches to Medical Device Cybersecurity (2016)
  - Premarket Guidance webinar (10/29/2014)
  - FDA/DHS workshop (2014)
  - Safety Communication to Stakeholders (2013)
  - Cybersecurity for networked medical devices shared responsibility (2009)
- **Organization**
  - Established CSWG of Subject Matter Experts (2013)
  - Established Cyber Incident Response Team under EMCM (2013)
  - Premarket Rounds – Cybersecurity (11/17/2014)
- **Information Sharing –** Helping to build an information sharing platform
  http://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

CDRH/FDA Collaborations led by EMCM[1]

- New partnership with **Department of Homeland Security**
  - Coordinating incident response with ICS-CERT
  - Participating in EO13636-PPD21 Integrated Task Force WGs
  - DHS-led Cyber-Physical Functional Exercise (Cracked Domain) planners and players
- Enhanced communication & partnering with **HHS**
  - Integrated Task Force (ITF)
  - HHS/Critical Infrastructure Protection
  - Cyber Threat Analysis Center (CTAC)
- Strengthen collaboration with **NIST** through standards and Cybersecurity Framework Working Group
- New collaboration with National Health Information Sharing and Analysis Center (**NH-ISAC)**
- Engaging proactively with **diverse stakeholders**
  - Outreach/education of hospital, healthcare & medical device community (users and industry)

[1]EMCM – Emergency Preparedness/Operations and Medical Countermeasures

Medical Device Interoperability and FDA

IVD Roundtable

Dharmesh Patel

June 2, 2016

Medical Device Interoperability Offers the Potential to Increase Efficiency in Patient Care

- Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices
  - ***Draft Guidance*** released January 2016

- Electronic medical devices are increasingly connected to each other and to other technology

Connected Systems Need to Safely and Effectively Exchange Information

- Design Considerations
  - Purpose of the Electronic Data Interface
  - Determine Anticipated Users
  - Risk Management
  - Verification and Validation
  - Labeling Considerations
  - Use of Consensus Standards

From “Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices”, DRAFT version January 26, 2016

Appropriate Documentation is Needed to Determine Safety and Effectiveness

- Contents of Pre-Market Submissions
  - Device Description
  - Risk Analysis
  - Verification & Validation
  - Labeling

From “Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices”, DRAFT version January 26, 2016

Contact Information

- Office of In vitro Diagnostics and Radiological Health (OIR)
  - Dharmesh Patel
    Dharmesh.Patel@fda.hhs.gov
  - digitalhealth@fda.hhs.gov
- Thank you!
- Questions?