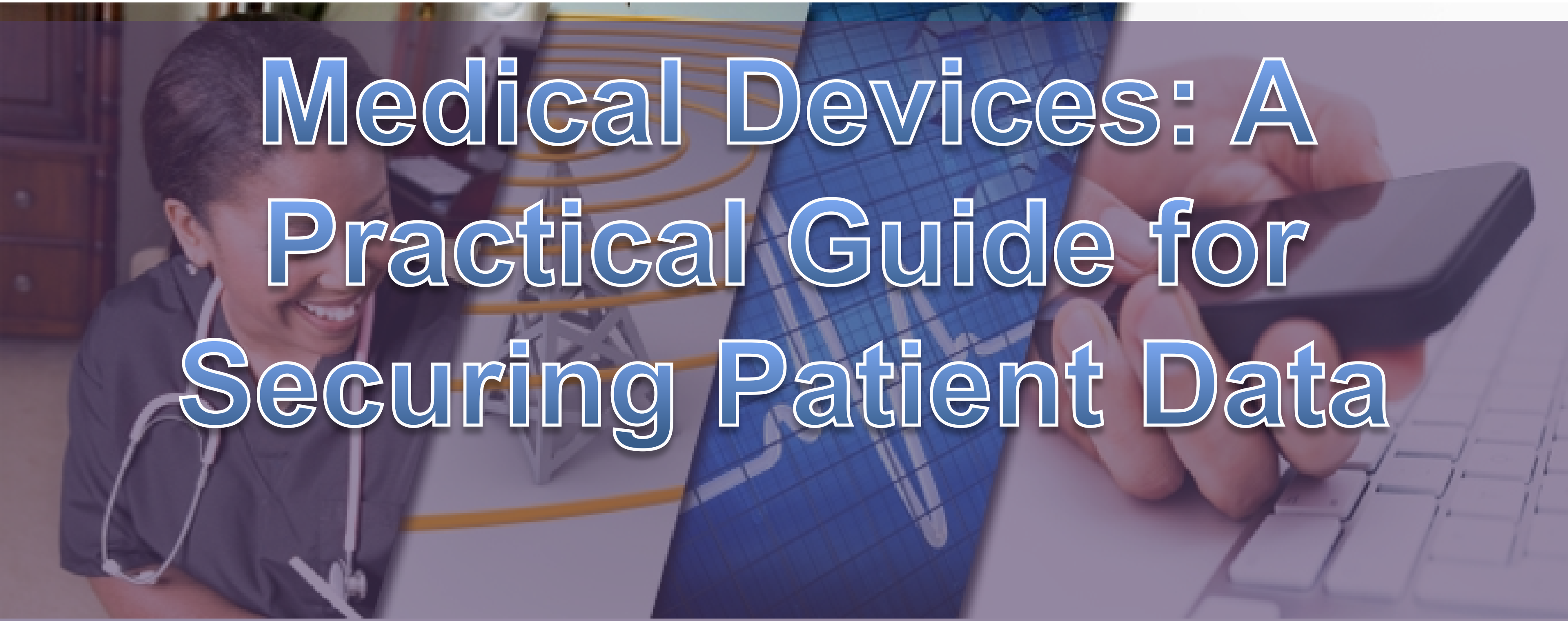


Medical Devices: A Practical Guide for Securing Patient Data

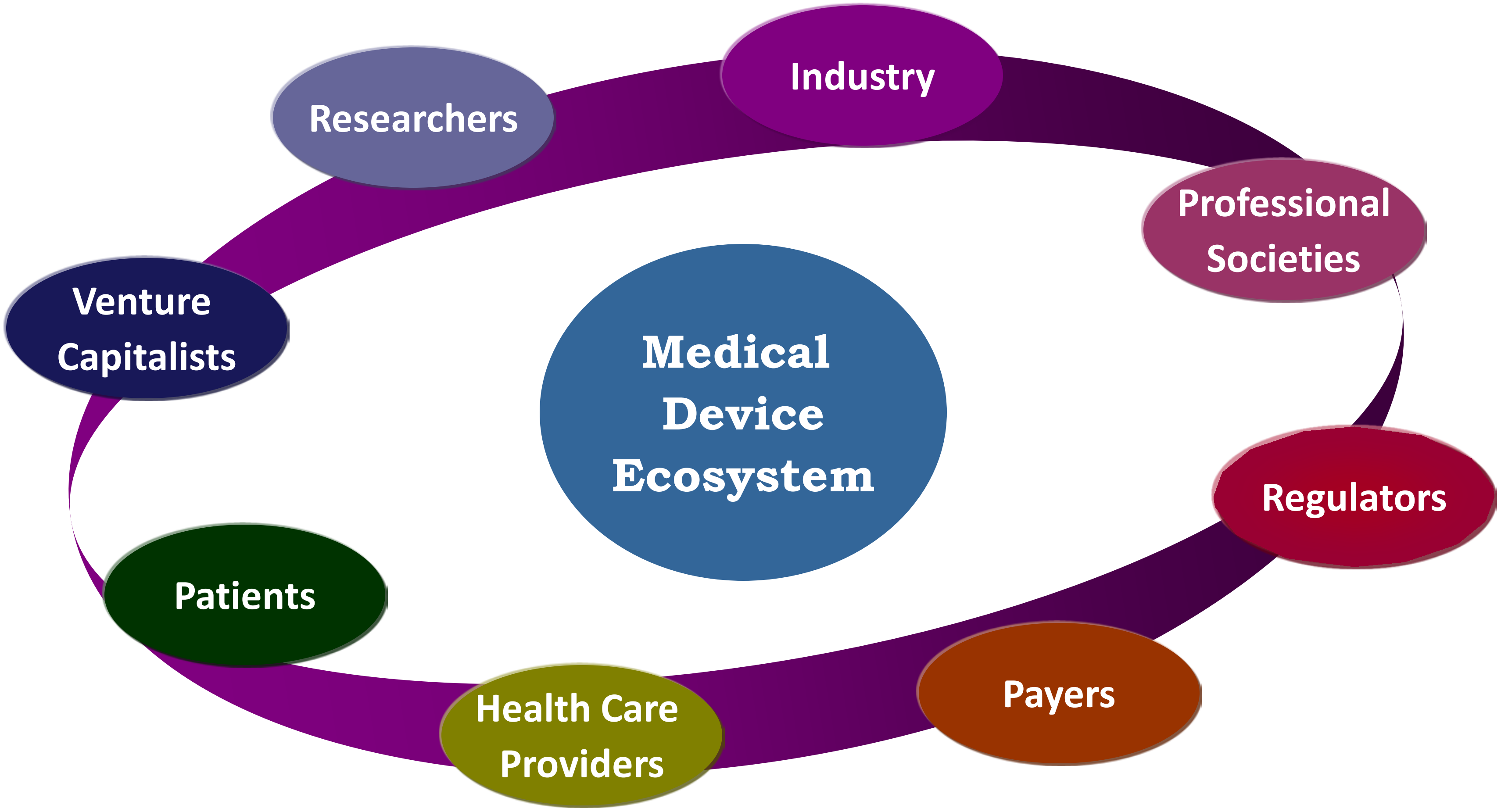
Safeguarding Health Information:
Building Assurance through HIPAA Security
HHS Office of Civil Rights and
National Institute of Standards & Technology
Tuesday September 23, 2014

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

September is National Preparedness Month

"Failing to prepare means preparing to fail"

Whole of Community Approach



Three Core Concepts

- Awareness

- Preparedness

- Collaboration

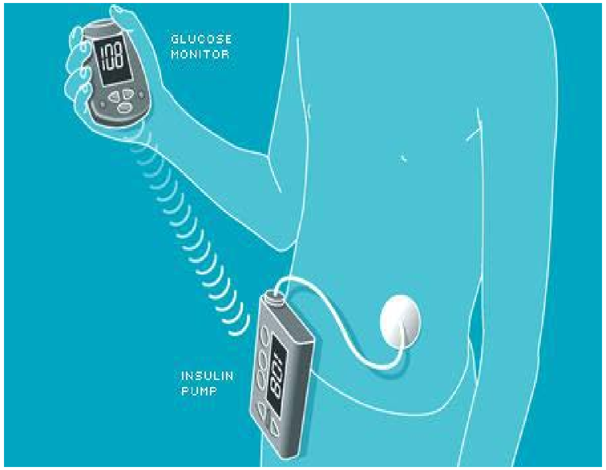
Roadmap for Today's Discussion

- Understanding the Current Landscape
- Our CDRH/FDA Medical Device Cybersecurity Program
- Our Vision Ahead

Scope of Public Health Impact

- 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

Medical Device Cybersecurity Background



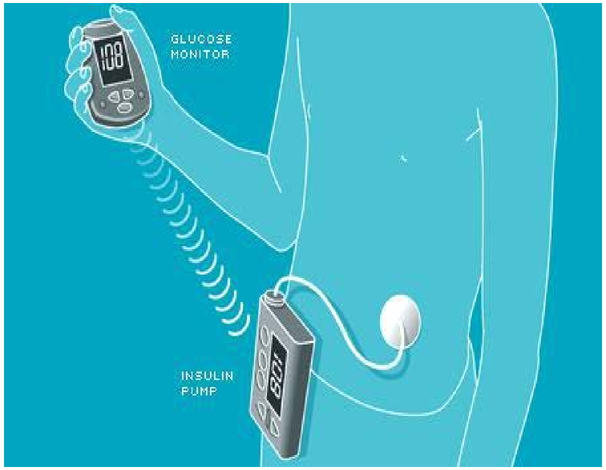
MEDICAL DEVICES

- Contain configurable embedded computer systems
- Increasingly interconnected
- Wirelessly connected
- Legacy devices

USE ENVIRONMENT

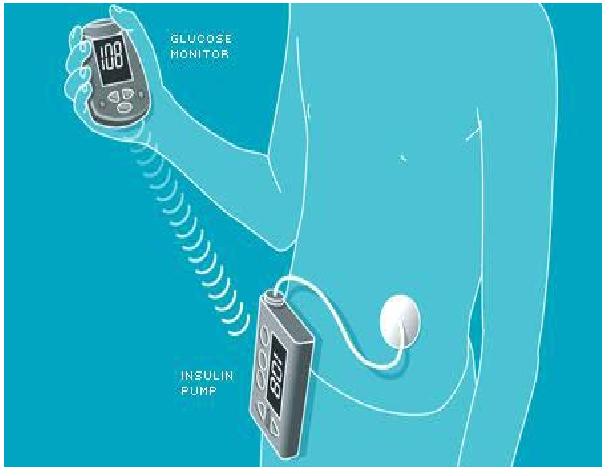
- Varied responsibilities for purchase, installation and maintenance of medical devices, often silo-ed
- Variable control over what is placed on the network
- Inconsistent training and education on security risks

Medical Device Vulnerabilities



- Network-connected medical devices infected or disabled by malware
- Malware on hospital computers, smartphones/tablets, and other wireless mobile devices used to access patient data, monitoring systems, and implanted patient devices
- Uncontrolled distribution of passwords
- Failure to provide timely security software updates and patches
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access

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 (Rios & McCorkle, 4/13)

CDRH/FDA Activities

- **Guidance**
  - Premarket (Draft, 2013)
  - Wireless Technology (2013)
  - CS for Networked Devices with OTS Software (2005)
- **Standards**
  - Cybersecurity (2013)
  - Interoperability (2013)
- **Public Communication**
  - Safety Communication to Stakeholders (2013)
  - 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

- 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**
  - HHS/Critical Infrastructure Protection
  - Cyber Threat Analysis Center (CTAC)
- Strengthen collaboration with **NIST** through standards and CSF Working Group
- Engaging proactively with diverse stakeholders
  - Outreach/education of hospital, healthcare & medical device community
- New collaboration with **NH-ISAC**

CDRH/FDA Ongoing Activities

Collaboration with Federal Partners

Premarket CS Expectations

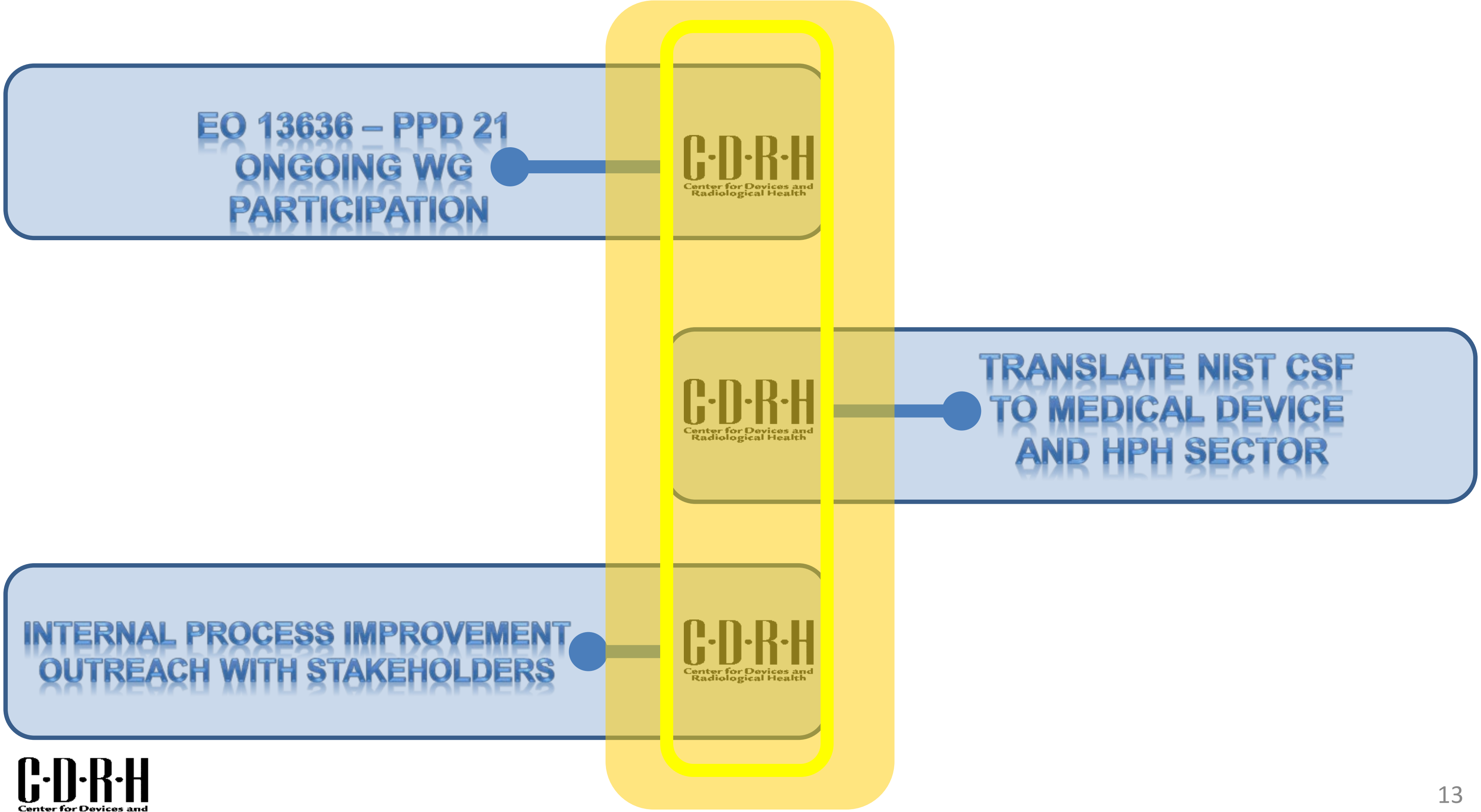
Maintaining Awareness Unintentional / Intentional Threats

Postmarket Surveillance

Stakeholder Engagement

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

Aligning with EO13636 & the Cybersecurity Framework for the HPH Sector



EO 13636 – PPD 21 ONGOING WG PARTICIPATION

TRANSLATE NIST CSF TO MEDICAL DEVICE AND HPH SECTOR

INTERNAL PROCESS IMPROVEMENT OUTREACH WITH STAKEHOLDERS

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

Save The Date!!

Public Workshop:

'Collaborative Approaches for Medical Device and Healthcare Cybersecurity'

October 21st-22nd 2014

National Intellectual Property Rights Coordination Center, Arlington, Va

More info: Suzanne.Schwartz@fda.hhs.gov