The National Medical Device Information Sharing & Analysis Organization (MD-ISAO) Initiative

Session 2, February 19, 2017

Moderator: Suzanne Schwartz, Assoc. Dir., CDRH, FDA

Denise Anderson, MBA, President, NH-ISAC

Dale Nordenberg, M.D., Executive Director, MDISS

NH-ISAC
NATIONAL HEALTH - ISAC

MDISS
MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM

Speaker Introduction

Denise Anderson, MBA

President

NH-ISAC

National Health Information Sharing and Analysis Center

Speaker Introduction

Dale Nordenberg, M.D.

Executive Director

MDISS

Medical Device Innovation, Safety and Security Consortium

Conflict of Interest

Panel participants have no real or apparent conflicts of interest to report.

Moderator

Suzanne Schwartz, MD, MBA, CDRH, FDA

Note: Moderator is only facilitating discussion of the content prepared and delivered by the speakers

Speakers

Denise Anderson, President, NH-ISAC

Dale Nordenberg, MD, Executive Director, MDISS

Note: Speakers prepared the content contained in this presentation

Learning Objectives

- Recognize the unique role of the NH-ISAC
- Discuss the science, technology, and epidemiological foundations to understand the difficulty in identifying and controlling malware
- Illustrate and discuss the open collaboration to enable cybersecurity information sharing
- Explain the FDA guidance and provided benefits of medical device manufacturers participating in an ISAO
- Identify key aspects of ISAO including the governance model for operations and data sharing

An Introduction of How Benefits Were Realized for the Value of Health IT

- Enabling the sharing of cyber-information
- Developing best practices for cyber-security solutions
- Creating new capabilities to collect and aggregate cyber information securely
- Improving data for treatments/clinical
- Securing electronic data
- Promoting patient and population safety
- Securing health innovations of medical devices

Agenda

- Medical Device Cybersecurity: The Public Health Challenge and Response
- FDA, NH-ISAC and MDISS Memorandum of Understanding
  - Collaboration initiatives and participation
  - Information sharing initiatives
    - MD-VIPER
    - National Medical Device Cyber Surveillance and Safety Network
- FDA guidance

Cyber-Risk: An 'Interesting Case'? Defining a Public Health Problem

Parameters Defining Public Health Importance	Assessment of Parameters	Impact Scoring
Breadth of exposure	• 1 Billion patient visits / year in USA • >100 B exposures to connected devices	++++
Potential severity of impact	Range of safety, privacy and business impacts include severe	++++
Preventability of adverse patient and institutional events	Engineering, policy, best practices, standards, regulatory science, etc. are able to substantially contribute to preventability	++++

Exposure

People

- 1 billion healthcare visits / year
- 1.5 M nursing home residents
- Home care

100 B Patient exposures to connected medical devices over 10 years

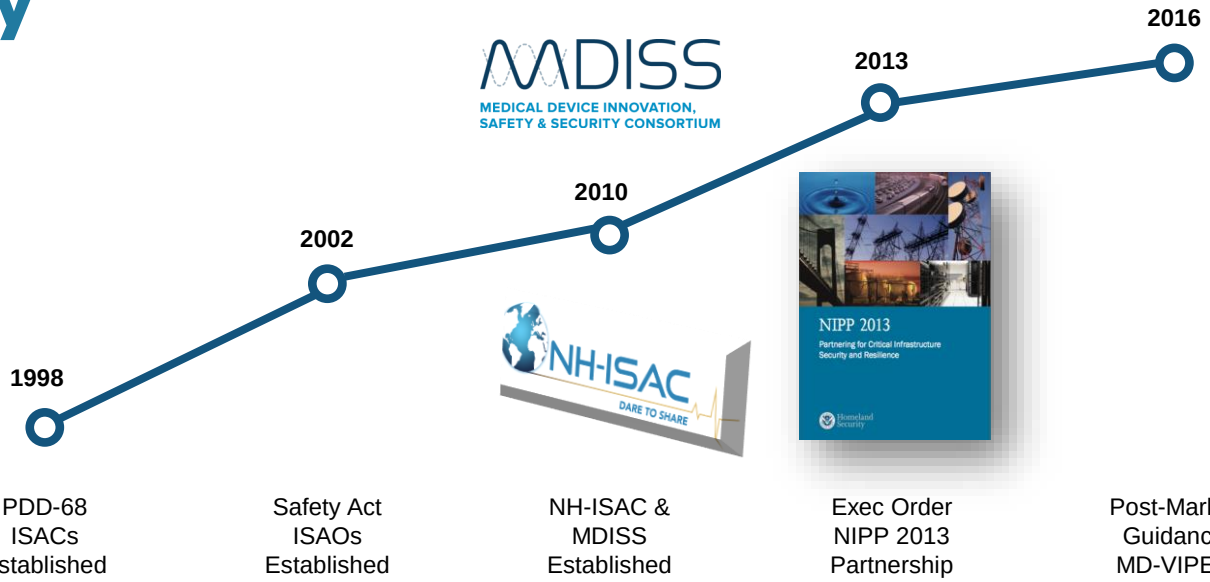
National Healthcare Technology Cyber Surveillance and Safety Network

Places

- 6,000 hospitals
- 17,000 nursing homes

- **Safety risk**
- **Privacy risk**
- **Business risk**
- **Regulatory risk**
- **Accreditation risk**
- **Reputational risk**
- **Professional liability risk**

Organizing Response Capability & Capacity



- The original ISACs are almost 20 years old
- Most ISACs are private sector formed and led
- ISACs are non-profit

NIPP – National Infrastructure Protection Plan

ISAC: Critical Infrastructure

- **Information Sharing and Analysis Centers (ISACs)**
- Operational entities **formed by critical infrastructure owners and operators**
- Gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure
- ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders

Source: Presidential Decision Directive 63, 1998

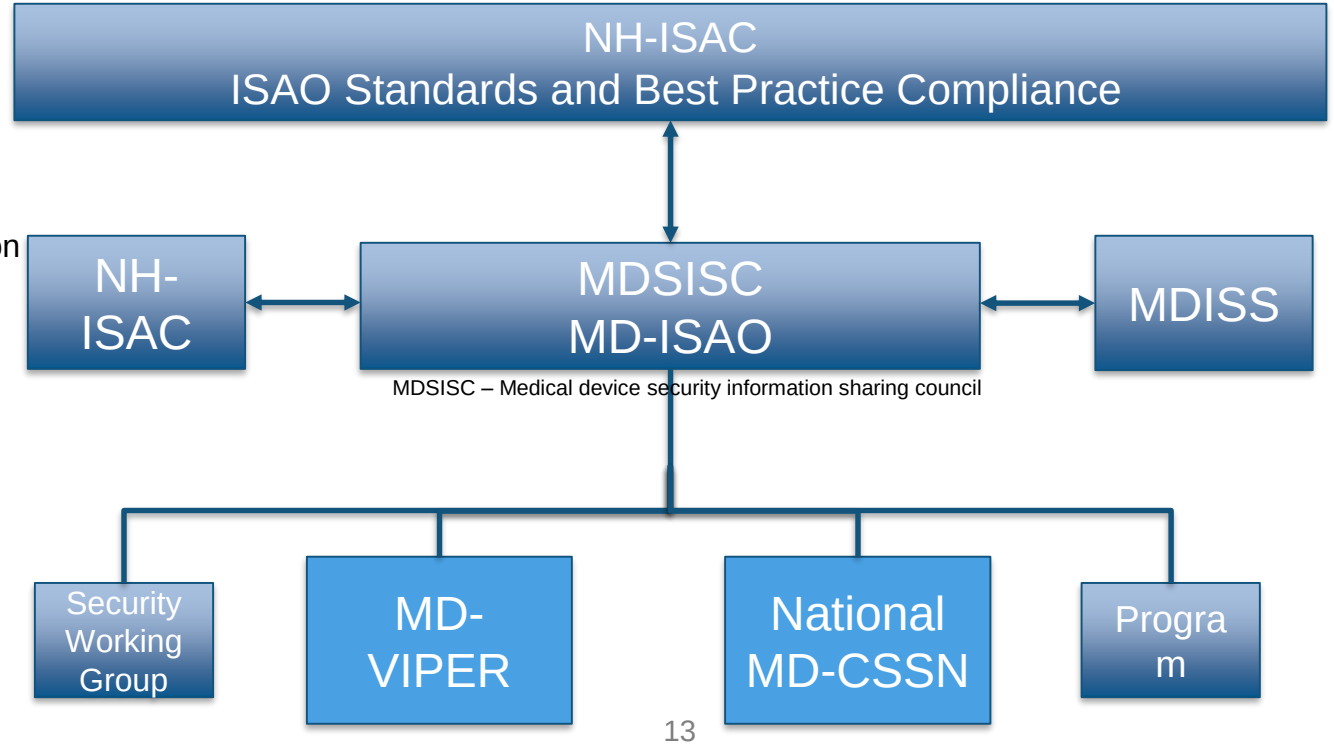
ISAO: Cyber-Information Sharing (General)

Information Sharing and Analysis Organization (ISAO)

- Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of:
  - Gathering and analyzing
  - Communicating or disclosing
  - Voluntarily disseminating
- *ISACs, which are actually a sector-based type of ISAO, are and will continue to be a vital piece of the U.S. information sharing effort. The expertise of existing ISACs will be vital during the ISAO standards development process. Once launched, the new ISAOs will be able to share information with ISACs, thus broadening each group's information sharing network.*

Source: https://www.dhs.gov/isao-faq

National Medical Device ISAO



- Cyber information sharing
- Critical infrastructure

- Public health
- Informatics
- Regulatory science
- Epidemiology

MDSISC – Medical device security information sharing council

MD-VIPER – Medical Device Vulnerability Intelligence Program for Evaluation and Response

MD-CSSN – Medical Device Cyber Surveillance and Safety Network

Memorandum of Understanding FDA – NH-ISAC – MDISS Collaborative Innovation and Response

- Create an environment that fosters **stakeholder collaboration and communication**
- Develop timely awareness of the Framework for Improving Critical Infrastructure Cybersecurity **(NIST CSF)**
- Develop innovative strategies to **assess and mitigate** cybersecurity vulnerabilities before hazard
- Build a **foundation of trust** within the HPH community
- Establish a mechanism by which information regarding **cybersecurity vulnerabilities and threats can be shared**

Information Sharing: Cornerstone of Cyber Safety Programs

Evidence….
is the cornerstone of prevention and response

MD-VIPER Objectives

- Deliver a medical device vulnerability information sharing evaluation and response service
- Support FDA postmarket cybersecurity in medical devices guidance
- Create open community of medical device cybersecurity stakeholders
- Promote a consensus & consistency of approach and process
- Contribute to medical device cybersecurity education and understanding
- Foster situational awareness of medical device threats, best practices and mitigation strategies

MD-VIPER
Conditions for Alternative Reporting to 21 CFR 806

- The manufacturer is an active participant in an ISAO (such as NH-ISAC)
- The manufacturer is conducting a correction/removal to address a cybersecurity vulnerability
- The cybersecurity vulnerability in question has not led to any known serious injuries or deaths
- The manufacturer will meet the timeline criteria for communicating to its customers and then validating and distributing the deployable fix such that the residual risk is brought to an acceptable level

MD-VIPER
Keep it Focused….Keep it Familiar

- Very focused to support the FDA *Postmarket Management of Cybersecurity in Medical Devices* guidance
- Operates consistent with current FDA reporting pathways
- Operates under umbrella of NH-ISAC
- Data sharing protections through CISA; the Cybersecurity Information Sharing Act (2015)
- What's different
  - Cyber-data
  - Information sharing through ISAO replaces CFR 806 FDA reporting

MD-VIPER
Participation and Sharing Control

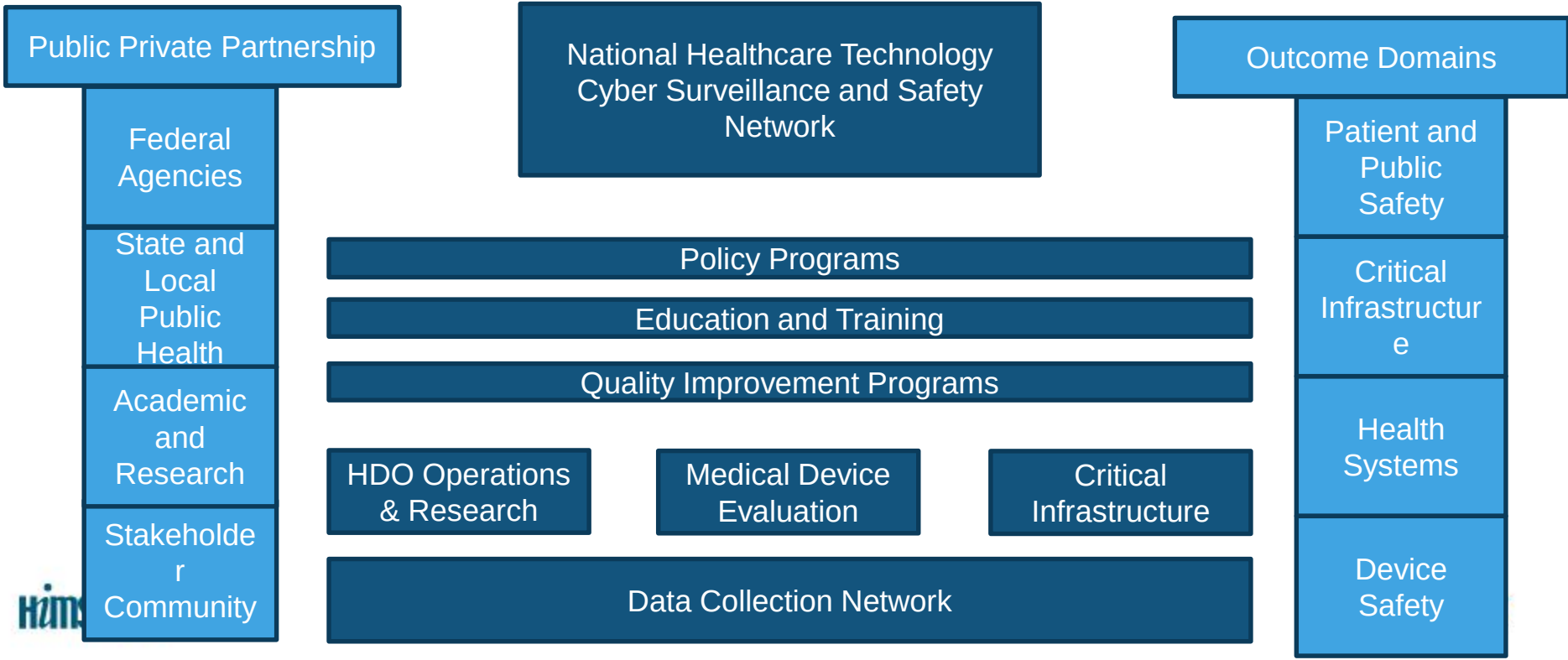
- Open to all medical device security stakeholders
- Free and voluntary*
- Tracking each event (submissions, data sharing event, communication event, etc.)
- Each information sharing event is triggered by the manufacturer
- Responsible sharing of information regarding vulnerabilities and threats in light of specified vulnerabilities for stakeholder awareness
- Participants have access to publically released data only – not access to the database

**Need to register and sign NDA*

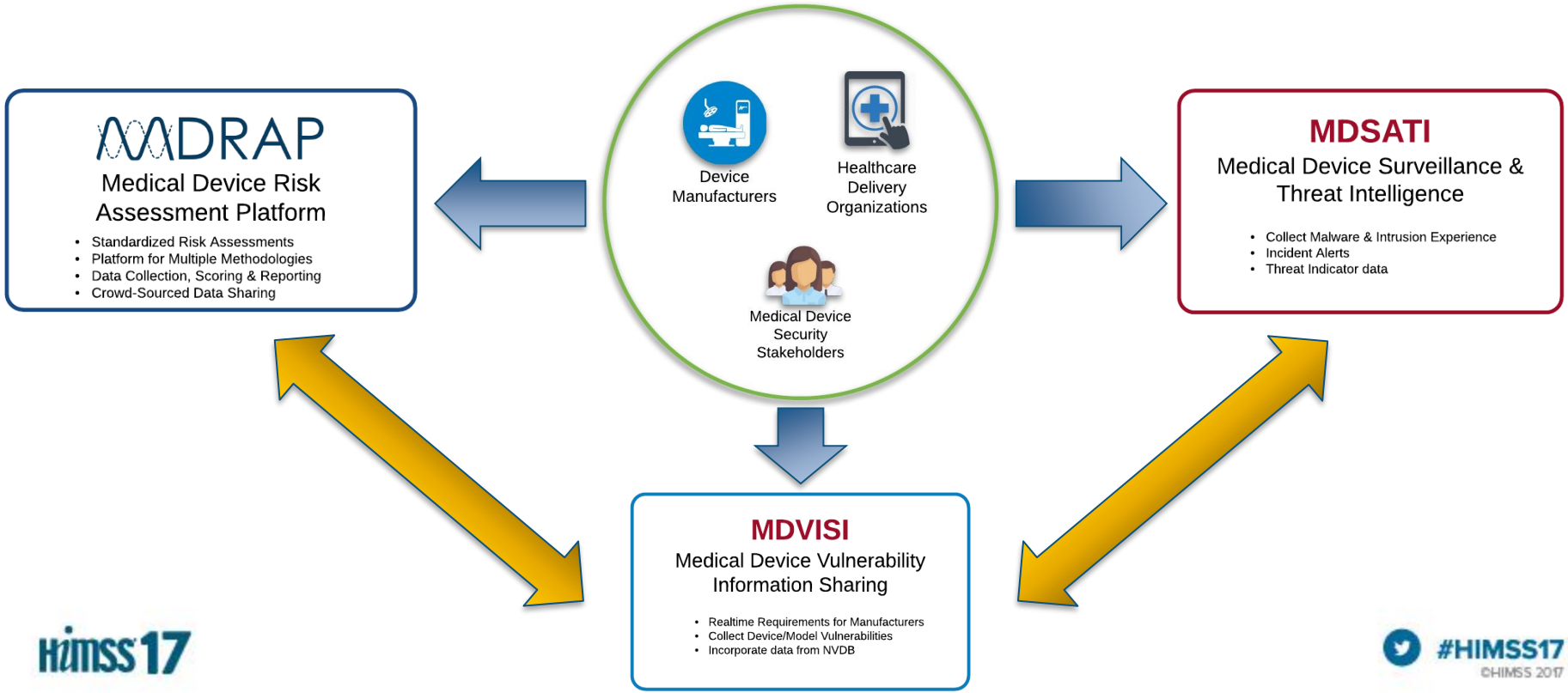
MD-VIPER Coordinated Disclosure

- MD-VIPER can support coordinated disclosure
  - Supports rapid collaborative review for validation
  - Provide mechanism for communicating timelines for mitigating controls to be developed
  - Disclosure to public occurs with mitigating controls for optimal safety based on coordinated disclosure best practices and standards
  - MD-VIPER will support communications between reporters of vulnerabilities and the manufacturers, if needed
- Foundations
  - National Telecommunications and Information Administration (NTIA)
  - ISO/IEC Standards
  - FDA Postmarket guidance

National Healthcare Technology Cyber Surveillance and Safety Network



National Cybersecurity Safety & Surveillance Network



Threat Intelligence (TI) – Many Challenges

- Diversity
  - Medical Devices
  - Manufacturers
  - Health systems
- Expert domains, e.g. clinical, cyber, biomed, safety, etc
- Sensitivity of data sharing
- Regulators
- Accreditation
- Defining threat intelligence
- Detection challenges
- Technology challenges
- Sharing at scale to create real TI value
- Absence of outcome or impact for context

A Summary of How Benefits Were Realized for the Value of Health IT

- Information sharing
- Collaborations between medical device manufacturers and health delivery organizations
- Creating new capabilities to collect and aggregate cyber information securely
- Creating important new insights
- Identifying and solving emerging complex cybersecurity challenges
- Promoting patient and population safety

Questions

For Specific Questions Related to the Postmarket Cybersecurity Final Guidance: AskMedCyberWorkshop@fda.hhs.gov

For General Questions about FDA and Medical Device Cybersecurity:
Suzanne.Schwartz@fda.hhs.gov
Seth.Carmody@fda.hhs.gov

Denise Anderson, MBA
President
National Health Information Sharing and Analysis Center (NH-ISAC)
contact@nhisac.org

Dale Nordenberg, MD
Executive Director
Medical Device Innovation, Safety and Security Consortium (MDISS)
dalenordenberg@mdiss.org