The Next Frontier in Medical Device Security

Session #76, February 21, 2017

Denise Anderson, President, NH-ISAC
Dr. Dale Nordenberg, Executive Director, MDISS
Speaker Introduction

Denise Anderson, MBA
President
National Health Information Sharing and Analysis Center (NH-ISAC)

Dale Nordenberg, MD
Executive Director
Medical Device Innovation, Safety and Security Consortium (MDISS)
Conflict of Interest

Denise Anderson, MBA
Dale Nordenberg, MD

Have no real or apparent conflicts of interest to report.
Agenda

• Learning Objectives
• NH-ISAC and MDISS Overview
• Medical Device Security Information Sharing Council (MDSISC)
• Medical Device Cybersecurity Information Sharing Initiative
• Medical Device Risk Assessment Platform (MDRAP)
• Medical Device Surveillance and Threat Intelligence
• Medical Device Vulnerability Intelligence Program for Evaluation and Response (MD-VIPER)
• Questions
Learning Objectives

• Explain the meaning and use of threat intelligence information
• Identify challenges for the collection of threat intelligence data for medical devices
• Explain medical device risk assessment approaches and how crowdsourcing assessments can accelerate cost-effective access to medical device risk assessments
• Explain the role of the NH-ISAC and how medical device stakeholders can securely contribute data to the NH-ISAC to promote device security, patient safety, and critical infrastructure protection
A Introduction of How Benefits Were Realized for the Value of Health IT

• Sharing information
• Collaborating
• Creating new capabilities to collect and aggregate cyber information securely
• Creating important new insights
• Identifying and solving emerging complex cyber security challenges
• Promoting patient and population safety
Who We Are

MDISS
MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM

NH-ISAC
NATIONAL HEALTH - ISAC
Medical Device Cyber Security: A Public Health Challenge
Over next 10 years

100 Billion Exposures

Between patients and connected medical devices

People
- 1 billion healthcare visits
- 1.5 M nursing home residents

Places
- 6,000 hospitals
- 17,000 nursing homes

RISKS
- Patient Care & Safety
- Privacy
- Operational
- Financial
- Reputational
- Compliance
Institute of Medicine (IOM) Health Care Quality AIMS

- Safe - Avoiding preventable injuries, reducing medical errors
- Effective - Providing services based on scientific knowledge (clinical guidelines)
- Patient centered - Care that is respectful and responsive to individuals
- Efficient - Avoiding wasting time and other resources
- Timely - Reducing wait times, improving the practice flow
- Equitable - Consistent care regardless of patient characteristics and demographics

Medical devices are a core component of healthcare quality
Three parameters define the importance of a public health problem:

- Breadth of exposure, e.g. incidence/prevalence
- Depth of impact, e.g. morbidity and mortality
- Preventability
New Digital Health Infrastructure Demands
New Best Practices

• The nation’s healthcare system operates on a national biomedical device network
• The connected care environment has evolved more rapidly than associated best practices
• The ‘health system’ has not adequately budgeted or committed to important practices needed to evolve and secure today’s health system infrastructure
  – Assessment of devices
  – Cyber security exercises
  – Monitoring
  – Updating and patching

Best Practices
Legacy-Drag
Key Public Health Messages for Cyber Safety

- Medical device cybersecurity is a public health challenge
  - Large scale
  - Multi-sector and multi-industry
  - Urgent assessment needs
  - Scalable solutions
  - Policy
  - Education and awareness
  - Collaborative solutions

- Transforming technology vulnerabilities and risk into healthcare delivery solutions
- Delivering patient centric security...and securing patient care delivery environments
Jurisdictional Chasms: Patient Safety Challenges

Stakeholders, priorities, policy, etc. varies by jurisdiction

<table>
<thead>
<tr>
<th>Focus Area</th>
<th>Oversight Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Safety</td>
<td>FDA</td>
</tr>
<tr>
<td>Hospital Safety</td>
<td>CMS, Accreditors, State Health Departments</td>
</tr>
<tr>
<td>Community/Critical Security</td>
<td>DHS, Law Enforcement Agencies</td>
</tr>
</tbody>
</table>
Brief History of Medical Device Cyber Security
Evolution of Medical Device Security

- Medical Device Regulation Act
- Safe Medical Devices Act
- HIPAA
- Medical Device User Fee and Modernization Act
- HITECH
- Insulin Pump Vulnerability
- HIPAA Final Rule
- FDA Draft Postmarket Guidance
- FDA Postmarket Final Guidance
- FDA Safety and Innovation Act
- MD-5VIPER Est. by NH-ISAC & MDISS
- MDSISC Est. by NH-ISAC & MDISS
- Defective Therac-25 Accelerators
- Medical Device Modernization Act
- Reigel vs. Medtronic
- NH-ISAC Founded
- MDISS Org. Established
- Pacemaker Hack
- FDA Premarket Guidance
- MD-5VIPER Est. by NH-ISAC & MDISS
- Medical Device User Fee and Modernization Act
- Reigel vs. Medtronic
- NH-ISAC Founded
- MDISS Org. Established
- Pacemaker Hack
- FDA Premarket Guidance
- MD-5VIPER Est. by NH-ISAC & MDISS
- Medical Device Modernization Act
- Reigel vs. Medtronic
- NH-ISAC Founded
- MDISS Org. Established
- Pacemaker Hack
- FDA Premarket Guidance
- MD-5VIPER Est. by NH-ISAC & MDISS
- Medical Device Modernization Act
- Reigel vs. Medtronic
- NH-ISAC Founded
- MDISS Org. Established
- Pacemaker Hack
- FDA Premarket Guidance
- MD-5VIPER Est. by NH-ISAC & MDISS
Information Sharing Activities
Information Sharing: Cornerstone of Cyber Safety Programs

Evidence is the cornerstone of prevention and response.
Medical Device Information Sharing Initiative

and

National Healthcare Technology Cyber Surveillance and Safety Network
Medical Device Security Information Sharing Council (MDSISC)

- Co-Chaired by NH-ISAC & MDISS
- Mission:
  - Engage stakeholders
  - Execute best practices for secure information sharing
  - Exchange information to promote efficient, secure and safe use of medical devices and associated networks
- MOU: FDA, NH-ISAC and MDISS
  - MD-VIPER
  - National Healthcare Technology Cyber Surveillance and Safety Network
- Current membership:
  - <100 individuals
  - >40 organizations
MDSISC Activities & Products

• Medical Device Security Information Sharing Initiative
• Listserv to share and exchange information
• Monthly meetings
• Threat briefings
• White papers on threats and best practices
• Medical device track at NH-ISAC summits
• Medical device security workshops
• Sub-groups focused on specific topics
Medical Device Security Information Sharing Initiative

- Press release June 2016
- Addresses global public health challenge of medical device cybersecurity and cyber safety
- Information sharing includes medical device risk assessments, host vulnerabilities and threat intelligence

June 2016 press release
NH-ISAC and MDISS Memorandum of Understanding with FDA

• Press release October 2016
• Addresses shared interest and collaboration around medical device cybersecurity

NH-ISAC and MDISS Sign Memorandum of Understanding (MOU) with FDA Around Collaboration of Medical Device Cybersecurity

A shared interest and collaboration in encouraging the identification, mitigation, and prevention of cybersecurity threats to medical devices fosters a MOU between NH-ISAC, MDISS and FDA.

Kennedy Space Center, FL, October 18, 2016 – The National Health Information Sharing and Analysis Center (NH-ISAC), the Medical Device Innovation, Safety and Security Consortium (MDISS), and the U.S. Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH) recently signed a MOU to collaborate in areas of mutual interest.

The goals of collaboration include the following:

Create an environment that fosters stakeholder collaboration and communication, and encourages the sharing of information about cybersecurity vulnerabilities that may affect the safety, effectiveness and security of the medical devices, and/or the integrity and security of the surrounding healthcare IT infrastructure;

Develop awareness of the Framework for Improving Critical Infrastructure Cybersecurity and enable HPH sector stakeholders to successfully adapt and operationalize the framework for their organizations and products;

Encourage stakeholders within the HPH Sector, to develop innovative strategies to assess and mitigate cybersecurity vulnerabilities that affect their products, and

Build a foundation of trust within the HPH community so that all healthcare technology and medical device stakeholders can directly benefit from the sharing of cybersecurity vulnerability- and/or threat information identified within the HPH Sector, as well as intelligence feeds from other Critical Infrastructure Sectors that may secondarily affect healthcare and the public health.

NH-ISAC & MDISS MOU with FDA
Medical Device Information Sharing Initiative Reporting: Keep it Familiar

• Very focused to support the FDA *Postmarket Management of Cybersecurity in Medical Devices* guidance
• Operates under umbrella of NH-ISAC and Cybersecurity Information Sharing Act (2015)
• Its new!
  – Type of data - cyber
  – Receiving entity – MD-VIPER
• Key operating design principles consistent with current FDA reporting pathways to help manufacturers easily adjust to this new reporting pathway
  – Website information provisioning format
  – Information
  – Data collection fields and forms
  – Explanation of how it relates to 806/803 reporting; recalls, enhancements, etc.
MD-VIPER Reporting
Conservation of Current Principles and Processes

• Manufacturers
  – Report vulnerabilities to MD-VIPER
  – Assess cyber vulnerabilities
  – Determine impact on safety and essential performance

• Coordinated disclosure
  – Integrated process for manufacturers
  – Mechanism for MD-VIPER to render vulnerabilities public

• MD-VIPER will support communications between reporters of vulnerabilities and the manufacturers, if needed
National Healthcare Technology Cyber Surveillance and Safety Network

Key Public Health Program Components

- Policy Programs
- Education and Training
- Quality Improvement Programs
- Analytics & Insights
- Data Collection
Medical Device Security Information Sharing Initiative

• Promote device security, patient safety and critical infrastructure protection
  – Medical Device Risk Assessment Platform (MDRAP)
  – Medical Device Surveillance and Threat Intelligence (MDSATI)
  – Medical Device Vulnerability Information Sharing (MDVISI)
Functional Activities

- Information Sharing Initiative
- Device evaluation
- Critical infrastructure protection
- Hospital operations
- Security requirements
Medical Device Risk Assessment Platform (MDRAP)

Risks are high priority to fix and not costly
- Higher likelihood
- Lower cost

Risks that may wait for remediation
- Lower likelihood
- Lower cost

Risks are high priority but costly to fix
- Higher likelihood
- Higher cost

Risks that may wait for remediation
- Lower likelihood
- Higher cost

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Level of Effort</th>
<th>Likelihood</th>
<th>Risk</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Logoff,</td>
<td>6</td>
<td>4.32</td>
<td>38.02</td>
<td>Automatic logoff capability is not present.</td>
</tr>
<tr>
<td>Audit Controls,</td>
<td>4</td>
<td>4.48</td>
<td>12.32</td>
<td>Audit trails (use logs) not produced.</td>
</tr>
<tr>
<td>Authorization,</td>
<td>7</td>
<td>1.15</td>
<td>8.1</td>
<td>Only the vendor can apply OS patches.</td>
</tr>
<tr>
<td>Cyber Security Product Upgrades,</td>
<td>8</td>
<td>0.9</td>
<td>1.98</td>
<td></td>
</tr>
</tbody>
</table>
Medical Device Vulnerability Information Sharing

• Coordinated disclosure
  – Supports rapid collaborative review for validation
  – Provide mechanism and times for mitigating controls to be developed
  – Disclosure to public occurs with mitigating controls for optimal safety
• Key References
  – National Telecommunications and Information Administration (NTIA)
  – ISO/IEC Standards
  – FDA Postmarket guidance
# Coordinated Disclosure: Case Studies

<table>
<thead>
<tr>
<th>Activity</th>
<th>St. Jude Medical</th>
<th>Johnson &amp; Johnson</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigating Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Residual Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordinated reviews</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outcome Quality</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
’Meaningful Security’
The Next Frontier!

NHSN Measures Endorsed by National Quality Forum (NQF)

The National Quality Forum (NQF) is a not-for-profit, nonpartisan, membership-based organization that works to catalyze improvements in healthcare. NQF endorsement is the gold standard for healthcare quality. NQF-endorsed measures are evidence-based and valid, and in tandem with the delivery of care and payment reform.

New! NQF NHSN Dialysis Event Bloodstream Infection (BSI) Measure Information October 2015 [PDF - 592 KB]
A Summary of How Benefits Were Realized for the Value of Health IT

- Sharing information
- Collaborating
- Creating new capabilities to collect and aggregate cyber information securely
- Creating important new insights
- Identifying and solving emerging complex cyber security challenges
- Promoting patient and population safety
Questions

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