apraciti

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

pillsbury

MARSH

Managing Cyber Risk in Life Sciences Technology

August 12, 2020

MARSH & McLENNAN COMPANIES

Welcome

Brian Finch
Partner
Pillsbury Winthrop Shaw Pittman LLP

Greg Garcia
Executive Director, Cybersecurity,
Health Sector Coordinating Council

Matthew McCabe
Senior Vice President
Marsh

Colin Morgan
Managing Director
Apraciti, LLC

Jessica Wilkerson
Cyber Policy Advisor, All Hazards Readiness,
Response, and Cybersecurity, Center for Devices
and Radiological Health, Food and Drug Administration

The Internet of Medical Things (IoMT)

- Electrocardiogram monitors.
- Cardiac defibrillators and pacemakers.
- Cochlear implants.
- Swallowable sensors to detect gastro-intestine conditions.
- Medication dispensing devices to manage proper dosage.
- Inventory management.
- Integration of personal devices.

Medical IoT to assess conditions such as high blood pressure, cholesterol, diabetes, heartbeat and weight gain.

Key Data Points (from HSCC)

95% of health care institutions confirm being **targeted for some form of cyberattack.**

$5.5+ billion

security breach costs in the health care industry every year.

There are over

7000

devices manufactured and smaller organizations are challenged with finding security talent for their product development.

There is a

62% increase in number of connected medical devices in 5 years which is expected to accelerate.

80%

of device manufacturers have less than **50 employees and need guidelines and help with security.**

Stakeholder Expectations Are Continuing to Evolve…

Patients

Patients expect lifesaving devices to be safe, secure, trustworthy, and free from breach.

Patient Safety & Data Privacy

Regulators

Regulators require cybersecurity throughout the total product lifecycle and ask for it during submissions.

Patient Safety

Customers

Health Care Delivery Organizations include comprehensive requirements in contract language and require ongoing security assessments.

Overall Risk Management

Along with the focus on risk.

Why Are Cybersecurity Risks Growing?

Medical technology is being built:

- with software
- using open source components
- to connect to hospital networks
- using Bluetooth, Wi-Fi, NFC
- in the cloud
- with machine learning
- and remote connectivity

Steps To Manage Risk

- Understand organizational strategy.
- Determine cybersecurity needs.
- Adopt an industry framework.
- Incorporate cybersecurity into the total-product-lifecycle.
- Establish risk assessment capabilities.
- Develop and implement program capabilities.

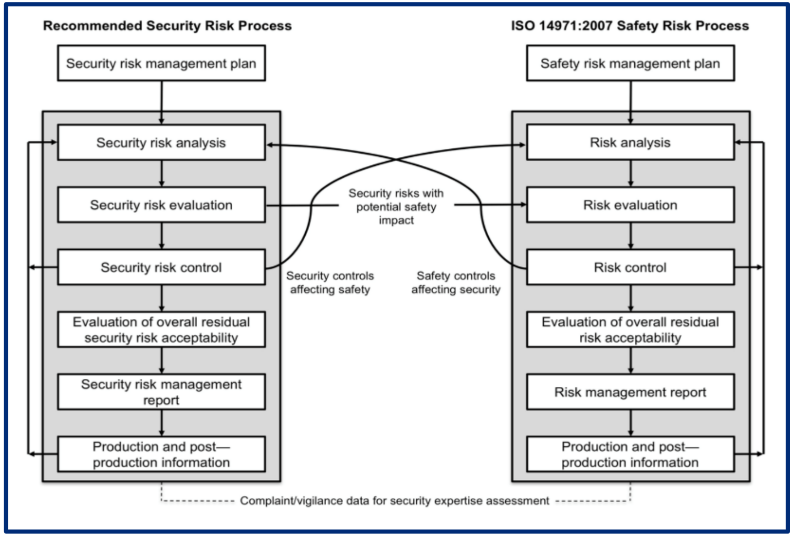
What are JSP key themes?

- **Design Control:** Building medical technology with cybersecurity standards and testing.
- **Compliant Handling:** Preparing and managing deployed medical technology cybersecurity.
- **Risk Management:** Assessing and responding to cybersecurity issues and events throughout the lifecycle of medical technology.
- **Maturity Evaluation:** Measuring and tracking progress of a cybersecurity program for medical technology.

Cybersecurity Risk Assessment

Figure – Evaluation of Risk of Patient Harm. The figure shows the relationship between exploitability and severity of patient harm, and can be used to assess the risk of patient harm from a cybersecurity vulnerability. The figure can be used to categorize the risk of patient harm as controlled or uncontrolled.

US FDA Postmarket Management of Cybersecurity in Medical Devices, 2016



AAMI TiR57

Can Any Laws Mitigate Connected Device Cyber Risks?

SAFETY Act?

- The law's protections apply to cyber products and services.
- Provides either immunity or a limit on damages, but only when there is an "act of terrorism."

PREP Act?

- Offers blanket immunity to FDA approved medical devices, drugs, and other items during a public health emergency.
- Immunity would apply in the case of cyberattacks on medical devices during an emergency.

SAFE TO WORK Act (proposed)

- No liability for health care providers unless plaintiffs can prove by "clear and convincing evidence" of
  1. gross negligence or willful misconduct by the health care provider; *and*
  2. that the alleged harm, damage, breach, or tort resulting in the personal injury was directly caused by the alleged gross negligence or willful misconduct.

Medical IoT (IoMT) is Part of U.S. Critical Infrastructure

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

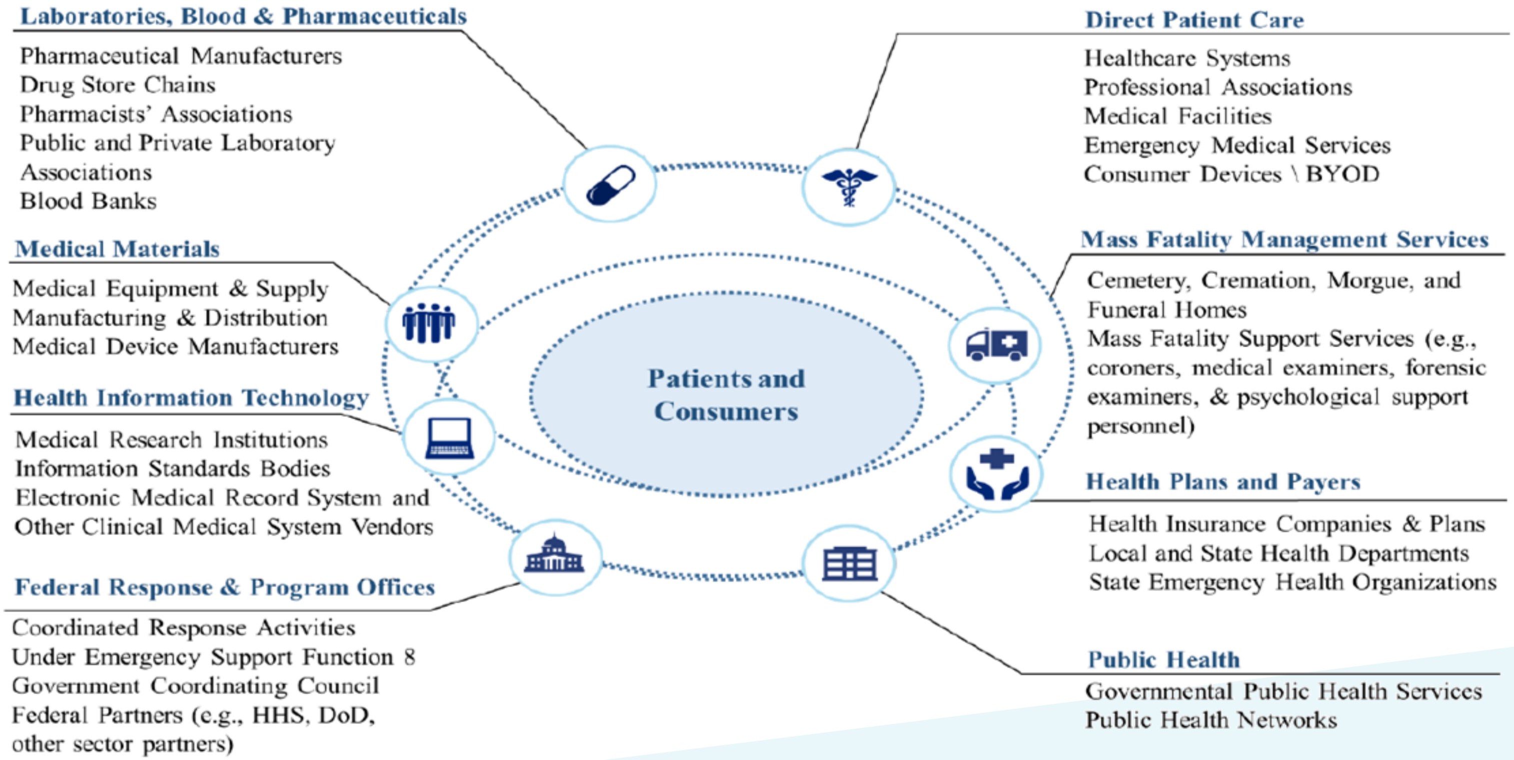
Critical Infrastructure

Systems and assets, whether physical or virtual, so vital to the United States that the[ir] incapacitation or destruction… would have a debilitating impact on security, … economic security, … public health or safety, or any combination of those matters.

§ 1016(e) of the USA Patriot Act of 2001
(42 U.S.C. § 5195c(e))

What is the Health Sector Coordinating Council?

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP



What is the HSCC Joint Cybersecurity Working Group?

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

- Largest standing Working Group under the HSCC umbrella, developing cross-sector policy and strategic approaches to mitigate major cybersecurity threats and vulnerabilities to the security and resiliency of the health care sector.
- 250 member organizations across the 6 health subsectors, 44 SME Advisors, 37 industry associations and professional societies, and 14 federal, state, local and Canadian government agencies. 578 member-organization personnel total.
- 15 outcome-oriented task groups meet regularly through the year; Full CWG meets twice a year around the country.
- Works closely on joint initiatives with:
  - HHS offices of Assistant Secretary for Preparedness and Response.
  - HHS Office of the Chief Information Officer.
  - Food and Drug Administration.

Given the Assignment

Health Care Industry Cybersecurity (HCIC) Task Force – June 2017
Six Imperatives and 105 Action Items

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks and exposure.
6. Improve information sharing of industry threats, risks, and mitigations.

Accepting the Challenge: HSCC Cybersecurity Task Groups

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

405(d) Health Industry Cybersecurity Practices

Supply Chain Cyber Risk Management

Future Gazing

Sub-group

Healthcare Technology Risk Analysis

Workforce Development

Medical Technology

Sub-groups

MedTech Legacy Devices

MedTech Model Contracts

MedTech Vulnerability Communications

Policy

Metrics for Cybersecurity Adoption

Telemedicine

International Engagement

Intellectual Data Protection

Risk Assessment

HSCC Cybersecurity Guidance Publications

See https://healthsectorcouncil.org/hscc-recommendations/

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

- **June 2020** — **Health Sector Return-to-Work (R2W) Guidance**
- **May 2020** — **Health Industry Cybersecurity Tactical Crisis Response**
- **May 2020** — **Health Industry Cybersecurity Protection of Innovation Capital**
- **March 2020** — **Health Industry Cybersecurity Information Sharing Best Practices**
- **March 2020** — **Management Checklist for Teleworking Surge During COVID-19**
- **October 2019** — **Health Industry Cybersecurity Supply Chain Risk Management**
- **October 2019** — **Health Industry Cybersecurity Matrix of Information Sharing Organizations**
- **June 2019** — **Health Industry Cybersecurity Workforce Guide**
- **January 2019** — **Medical Device and Health IT Joint Security Plan (JSP)**
- **January 2019** — **Health Industry Cybersecurity Practices (HICP)**

Thank You.
Questions?

Brian Finch
Pillsbury Winthrop Shaw Pittman LLP
Brian.Finch@PillsburyLaw.com

Greg Garcia
Health Sector Coordinating Council
Greg.Garcia@HealthSectorCouncil.org

Matthew McCabe
Marsh
Matthew.P.McCabe@Marsh.com

Colin Morgan
Apraciti, LLC
Colin.Morgan@Apraciti.com

Jessica Wilkerson
All Hazards Readiness, Response, and Cybersecurity,
Center for Devices and Radiological Health,
Food and Drug Administration

apraciti

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

pillsbury

MARSH JLT SPECIALTY