Health Care Cybersecurity Preparedness and Response for the Enterprise and Industry

Greg Garcia
Executive Director
Health Sector Coordinating Council Cybersecurity Working Group

Lisa Bisterfeldt
Cyber Resiliency Program Manager
St. Luke's Health System

California Hospital Association

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Sector Coordinating Council Cybersecurity Working Group

Presentation to the California Hospital Association
2023 Disaster Planning Conference
October 4, 2023

Health Care Cybersecurity Preparedness and Response

Greg Garcia
HSCC Cybersecurity Working Group Executive Director

Lisa Bisterfeldt
Cyber Resiliency Program Manager
HSCC OCCI Task Group Co-Author
St. Luke's Health System

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

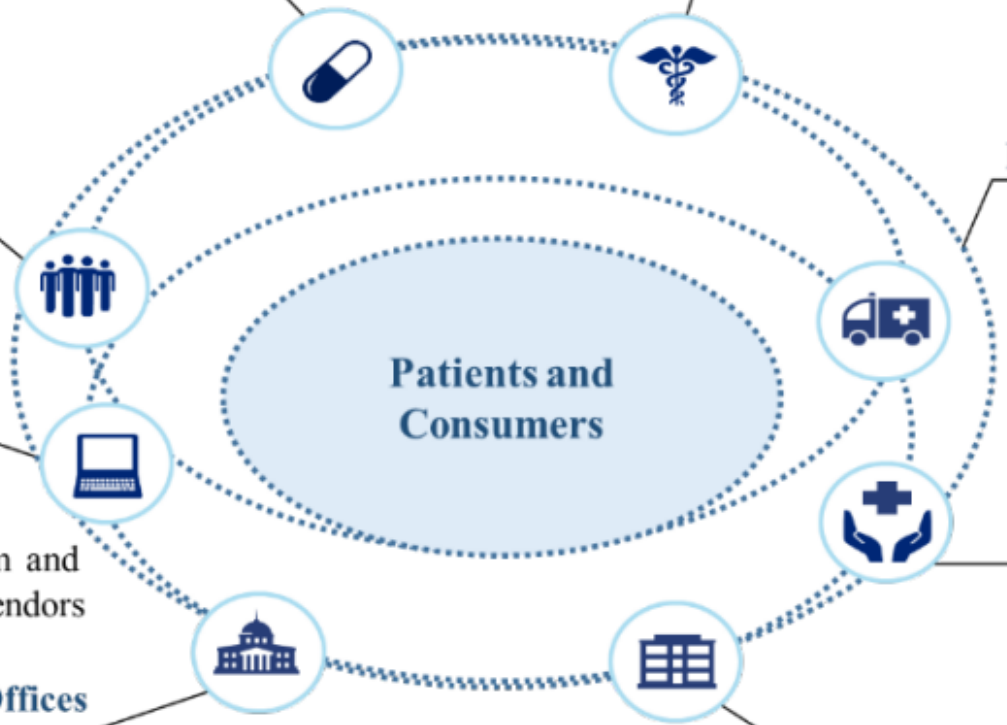
The Health Care Industry is Critical Infrastructure

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))

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

The Interconnected Healthcare Ecosystem



Laboratories, Blood & Pharmaceuticals

Pharmaceutical Manufacturers
Drug Store Chains
Pharmacists' Associations
Public and Private Laboratory Associations
Blood Banks

Medical Materials

Medical Equipment & Supply Manufacturing & Distribution
Medical Device Manufacturers

Health Information Technology

Medical Research Institutions
Information Standards Bodies
Electronic Medical Record System and Other Clinical Medical System Vendors

Federal Response & Program Offices

Coordinated Response Activities Under Emergency Support Function 8 Government Coordinating Council
Federal Partners (e.g., HHS, DoD, other sector partners)

Direct Patient Care

Healthcare Systems
Professional Associations
Medical Facilities
Emergency Medical Services
Consumer Devices \ BYOD

Mass Fatality Management Services

Cemetery, Cremation, Morgue, and Funeral Homes
Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

Health Plans and Payers

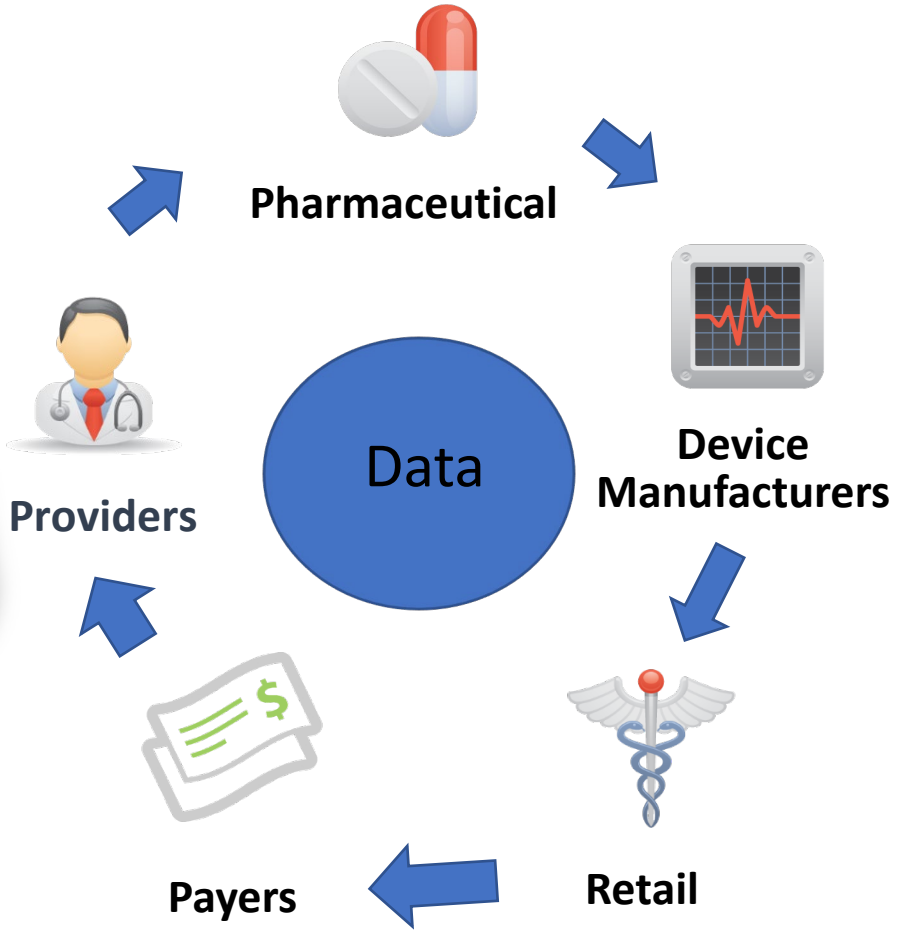
Health Insurance Companies & Plans
Local and State Health Departments
State Emergency Health Organizations

Public Health

Governmental Public Health Services
Public Health Networks

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

The Health Care Ecosystem – Connected, Digitized and Portable



Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cyber Pandemic in the Health Sector
Data Breaches

HHS Office for Civil Rights, which enforces the Health Insurance Portability and Accountability Act (HIPAA) data breach reporting:

- Healthcare data breaches of 500 or more records (name, address, medical, and financial records) increased from 329 to 715 between 2017 and 2021, with the number of individuals affected ranging between 20 million and 50 million
- In 2022, there were 707 data breaches, more than half of which occurred against third-party Business Associates
- Of the 52 million data records exposed in 2022, 43.9 or 84% were caused by hacking

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cyber Pandemic in the Health Sector: Ransomware

Journal of the American Medical Association (JAMA), from 2016 to 2021:

- 374 ransomware attacks on US healthcare delivery organizations exposed the protected health information of nearly 42 million patients.
- The annual number of ransomware attacks more than doubled from 43 to 91.
  - Almost half of ransomware attacks disrupted the delivery of health care, with common disruptions including:
    - electronic system downtime
    - cancellations of scheduled care
    - ambulance diversion

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cyber Pandemic in the Health Sector: Ransomware (cont.)

Journal of the American Medical Association (JAMA), from 2016 to 2021:

- Ransomware attacks on healthcare delivery organizations increasingly are:
  - Affecting large organizations with multiple facilities
  - Exposing the PHI of more patients
  - Less likely to be restored from data backups
  - More likely to exceed mandatory reporting timelines, and
  - Increasingly associated with delays or cancellations of scheduled care

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cyber Pandemic in the Health Sector Costs

IBM Cost of a Data Breach 2022 report:

- For the 12th year in a row, the health sector had the highest costs for a data breach, followed by
  - Financial
  - Pharmaceuticals
  - Technology
  - Energy
- The average breach cost in health care increased by nearly $1M and is now $10.1M
- Costs have also increased by over 40% in the last two years

Medical Device Risks

A patient bed has an average of 15 medical devices.
A 500 bed hospital could have **7,500 devices** . Most of them **connect to the network**.

- Most hospitals have 'networked' medical devices over 8-10 years old.
- The security-related components in these devices pose a cyber risk
  - The operating systems and microcontrollers no longer receive maintenance or security patches from the component vendor i.e. "Not Supported by Vendor"
  - Often have common passwords set by the manufacturer that cannot be changed.
  - Often have unencrypted hard drives
- Time and cost to update these devices is very expensive

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cybersecurity Attacks in Health Care

NEWS

'We weren't ready' — Inside St. Michael Medical Center during October cyberattack outages

THE CYBERSECURITY 202

An 'unprecedented' hospital system hack disrupts health-care services

Doctor says IT downtimes 'recipe for disaster' for ER patient care

CommonSpirit Health Suffers IT Outages, EHR Downtime at Multiple Hospitals

Multiple hospitals within the CommonSpirit Health system, one of the nation's largest nonprofit healthcare systems, are reporting IT outages and EHR downtime.

UVM Health Delays Epic EHR Implementation After Cyberattack, COVID-19

One of 2020's worst cyberattacks resulted in UVM Health delaying its Epic EHR implementation schedule.

Cyberattack Hits Brooklyn Hospitals That Serve Poor New Yorkers

Since late November, medical professionals have been using pen and paper as experts work to get the facilities fully back online.

LOCAL NEWS

St. Joseph's/Candler outage continues after ransomware attack

HEALTH

MercyOne sites open but online scheduling canceled after national cyberattack

'Just a crazy day': More than 30 systems hit by major network crash at The Ottawa Hospital

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.

LOCAL NEWS

Settlement: Scripps Health agrees to pay $3.5 million to patients affected in 2021 data breach

Nearly 1.2 million current and former patients at Scripps had their information compromised in the May 2021 ransomware attack.

Ransomware attack delays patient care at hospitals across the U.S.

CHI Memorial Hospital in Tennessee, some St. Luke's hospitals in Texas and Virginia Mason Franciscan Health in Seattle all have announced they were affected.

St. Anne Hospital in Burien suffering outages due to recent IT hacking incident

6 FEB 2023 NEWS

Major Florida Hospital Shuts Down Networks, Ransomware Attack Suspected

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cybersecurity Objectives

CWG Task Groups were formed to implement the

<u>2017 Healthcare Industry Cyber Security Task Force Imperatives</u>:

1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase healthcare 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

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cybersecurity Events = Extended Downtimes

Why Health Care

- **Reliance on technology creates vulnerability**
- **Limited preparedness for large scale cybersecurity attacks**
- **Operating in downtime creates increased risk**

Common Impacts

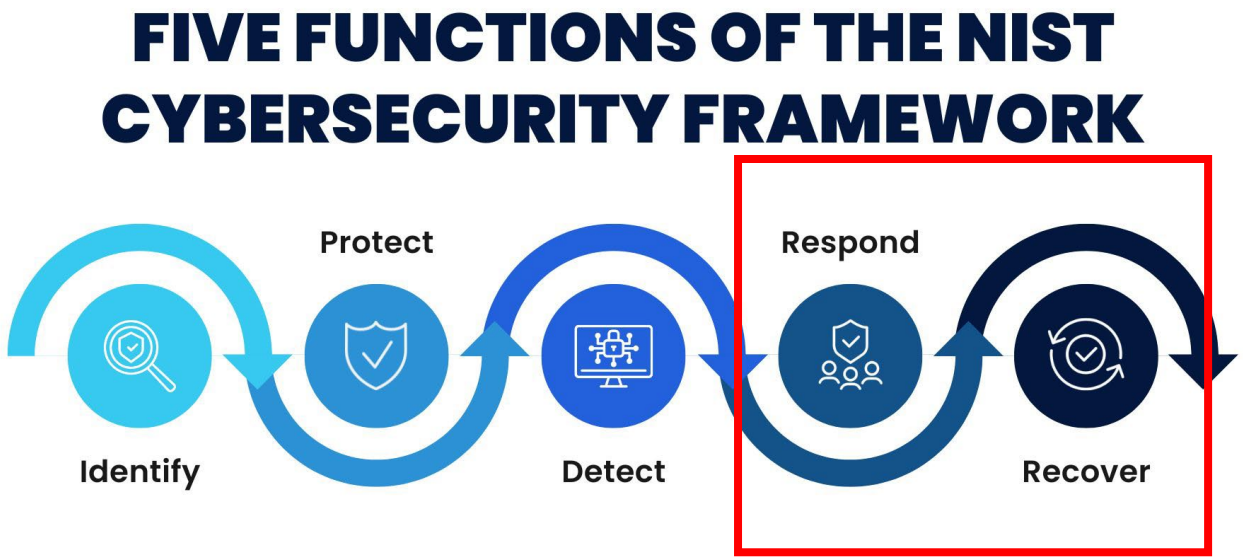
- **Limited executive support for cyber security and downtime preparedness**
- **1-2 weeks complete network outage**
- **Average time without electronic medical record - 21 days**
- **Downtime processes insufficient to support extended outage**

Network Dependency

- **Documentation**: EMR, procedure orders, patient education,
- **Priority Applications:** pharmaceuticals, imaging, cardiac monitoring, etc.
- **Resources:** supply movement, printers, telephones, email

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

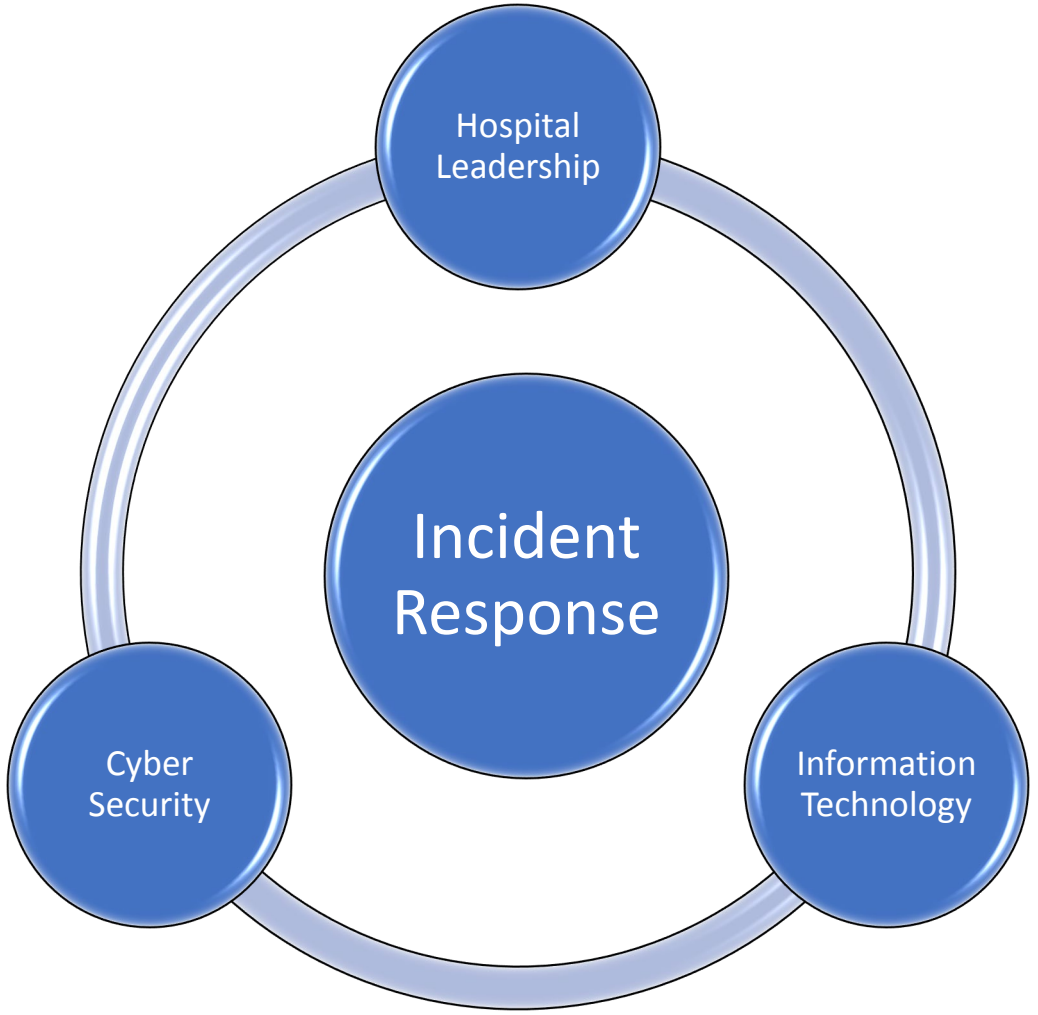
Emergency Management & Cybersecurity Response



Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Coordinated Healthcare Incident Response Plan (CHIRP)

- Plan a template to guide the response to a large-scale cybersecurity incident
- Platform to unite Cyber Security / Information Technology response plans and Hospital EOP's
- Leveraged as a stand-alone document or a supporting document to other supplemental plans
- Available here: HIC-CHIRP-FINAL_1.pdf (healthsectorcouncil.org)



Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Operational Continuity – Cyber Incident (OCCI) Checklist

The intent of this OCCI Checklist is to provide organizations of all sizes with key actionable and vetted steps that can be put into place at the first sign of a cybersecurity incident.

Action Driven

Provides Operational Tasks for the first 0-8 hours of an incident

Scalable

Applicable for all healthcare settings

Critical Access to Large Health Systems

Role Based

Aligned with the Hospital Incident Command System

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

OCCI Elements

Editable Collection of Incident Response Guides

Priority actions for the first 8 hours of a large-scale Cyber Security Event

Actionable items that allows HICS respond quickly

Available here: [Operational Continuity – Cyber Incident (OCCI) - Health Sector Council]

Version 2.0 released soon through partnership between HSCC and 405(d) Program and HHS

Response Guideline

Cybersecurity/Technology System Prolonged Massive Disruption or Outage

This checklist outlines recommended initial (first 12 hours) actions and considerations during cybersecurity incidents

Command positions should be activated as they are needed. If a command position is not activated, actions fall to the Incident Commander and can be delegated as appropriate. Position activation may depend on staff availability or the size and scope of the incident.

Based on assessment by CIO, CISO, and senior leadership, incident command may be activated Threshold for activation:

A prolonged massive disruption meets or has the potential to meet any of the following:

a. Patient safety and/or member service impacts
b. Large-scale clinical workflow, patient care, and/or member service impacts
c. Implementation of preventative defenses that could impact clinical workflow

	Incident Commander Role: Provides overall strategic direction on all site-specific response actions and activities.
1.1	Identify Incident scope and obtain situational awareness • Identify Scope – One site/multiple sites/Isolated outage/full network outage ○ Assume it is a malicious (cybersecurity) incident until proven otherwise • Situational awareness – operational, business, and clinical impacts
1.2	Establish a cadence and process for coordination with IS/IT and Cyber Security • Consider command center coordination or unified command based on organizational structure *(Hospital, IS/IT, and Cybersecurity Command)*
1.3	Activate applicable continuity and downtime plan(s) • If plans do not exist or are not functional, rapidly identify critical services and create a plan to continue/sustain services
1.4	Communicate activation of downtime plans to inform operational changes • Consider use of overhead paging, mass notification system, etc.
1.5	Approve recommendations from Operations relative to: • Scaling services • Pausing services • Initiating diversionary status
1.6	Address incident need by activating additional resources
1.7	Understand upstream and downstream impact(s) to partner organizations. Communicate as appropriate. • Community Connect • Other health systems • Community partners (e.g., SNF, LTAC, EMS)
1.8	Establish cadence for ongoing impact assessment and briefing (e.g., operational periods)

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

The Joint Commission on Cybersecurity

Sentinel Event Alert

A complimentary publication of The Joint Commission
Issue 67, Aug. 15, 2023

Preserving patient safety after a cyberattack

1. Evaluate HVA findings and prioritize hospital services that must be kept operational and safe for an extended downtime.
2. Form a downtime planning committee to develop preparedness actions and mitigations, with representation from all stakeholders.
3. Form a downtime planning committee to develop preparedness actions and mitigations, with representation from all stakeholders.
4. . Designate response teams.
5. Train team leaders, teams, and all staff on how to operate during downtimes.
6. Establish situational awareness with effective communication throughout the organization and with patients and families.
7. After an attack, regroup, evaluate, and make necessary improvements.

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Sector Coordinating Council (HSCC)

Organize

Collaborate

Promulgate

By the Sector for the Sector

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Sector Coordinating Council (HSCC)

- The cross-sector industry coordinating body representing one of 16 critical infrastructure sectors recognized under national policy
- A trust-community partnership convening health providers, companies, non-profits, and industry associations across six subsectors
- Serves as a special "Critical Infrastructure Partnership Advisory Council" to the government, exempt from normal public notification and participation requirements of the Federal Advisory Committee Act, given sensitive homeland security deliberations
- ***Mission: to identify cyber and physical risks to the security and resiliency of the sector, develop guidance for mitigating those risks, and work with government to facilitate threat preparedness and incident response***
- Focused on longer-term critical infrastructure policy and strategy, complementing the operational activities of the Health Information Sharing and Analysis Center

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HSCC Cybersecurity Working Group (CWG)

- Largest standing Working Group under the HSCC umbrella
  - 404 private-sector member organizations, including:
    - 47 industry associations
    - 54 non-voting Advisor firms
  - 18 Government organizations, including 11 federal agencies, 3 state agencies, 2 city agencies, and 2 Canadian
  - Total representing personnel: 922
- Identifies and develops strategic, cross-sector solutions to cybersecurity threats and vulnerabilities affecting the security and resiliency of the healthcare sector
- Outcome-oriented task groups meet regularly throughout the year; Full CWG meets twice a year around the country
- Works closely on joint initiatives with:
  - HHS Administration for Strategic Preparedness and Response
  - HHS Office of the Chief Information Officer
  - Food and Drug Administration

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2023 Executive Committee

CHAIR: Erik **Decker, VP - Chief Information Security Officer, Intermountain Healthcare**

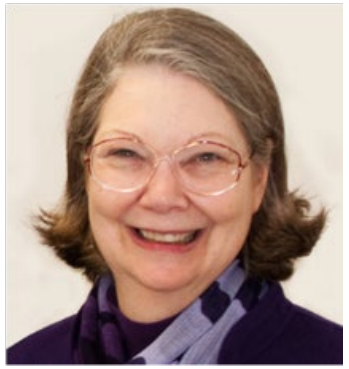
VICE CHAIR: Chris Tyberg, Chief Information Security Officer, Abbott

Julian Goldman, MD, Medical Director, Biomedical Engineering, Mass General Brigham

Samantha Jacques, Vice President Corporate Clinical Engineering, McLaren Healthcare

Leslie A. Saxon, MD, Executive Director, USC Center for Body Computing

Janet Scott, Vice President, Business Technology Risk Management and CISO, Organon



Leanne Field, PhD, M.S. Clinical Professor & Founding Director, Public Health Program, The University of Texas at Austin

Denise Anderson, President & CEO, Health Information Sharing & Analysis Center

Jonathan Bagnall Head of Cybersecurity, Digital Service & Solutions – Medical Technology, (CE), Fresenius Medical Care

Dr. Adrian Mayers, Vice President, Chief Security Officer, Premera Blue Cross

Sanjeev Sah, Vice President, Chief Security Officer, Centura Health

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Task Groups 2023

- **405(d) HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)**

Ongoing enhancement of 405(d) HICP resources

- **5-YEAR PLAN**

Update the Health Care Industry Task Force (HCIC) recommendations as a five-year plan reflecting emerging threat scenarios in a rapidly evolving healthcare system

- **INCIDENT RESPONSE - BUSINESS CONTINUITY**

Develop a healthcare cyber incident response and business continuity plan aligned with existing physical incident response protocols. The first publication on emergency management after the extended cyber-related outage was released in April 2022; the second publication on enterprise incident response plan imminent

- **MEASUREMENT**

Developing methodology for health sector-specific cybersecurity performance goals.

- **POLICY**

Activates as needed for policy proposals and response

- **MEDTECH CONTRACT LANGUAGE**

Updating Model Contract for Cybersecurity MC2) first published March 2022

- **MEDTECH SECURITY DEVELOPMENT (JOINT SECURITY PLAN UPDATE - JSP2)**

Published Medical Device and Health IT Joint Security Plan (JSP); and benchmarking report. Developing updated JSP2.

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Task Groups 2023 (cont.)

- **MEDTECH VULNERABILITY COMMUNICATIONS**

Provide guidance on preparing, receiving, and acting on medical device vulnerability communications. The first publication on patient awareness was released in April 2022. The second version of HDO preparedness is in process.

- **OPERATIONAL TECHNOLOGY MANUFACTURING SECURITY**

Develop best practices guide for securing OT manufacturing networks for healthcare manufacturing subsectors.

- **OUTREACH & AWARENESS**

Develop tools and strategies for enhancing visibility and messaging the imperative of healthcare cybersecurity, HSCC CWG, and its resources.

- **PRIVACY-SECURITY COLLABORATION**

Facilitate the interdependence of security and privacy risk to confidentiality, integrity, and availability of entity systems, data, etc., in patient safety and care.

- **PUBLIC HEALTH**

Identify strategies for strengthening the cybersecurity and resilience of SLTT public health agencies with the support of private sector and academic organizations.

- **RISK ASSESSMENT**

Published with HHS the NIST Cyber Framework Implementation guide; follow-on marketing and effort to measure adoption

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HSCC CYBERSECURITY WORKING GROUP
Publications, 2019-2023

SEE: https://healthsectorcouncil.org/hscc-publications

2023

- *Reprint* Tactical Crisis Response Guide
- *Updated* Updated Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)
- *Updated* Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)
- Coordinated Healthcare Incident Response Plan
- Recommended Government Policy & Programs
- Hospital Cyber Landscape Analysis (Joint HSCC/HHS)
- Prioritized Recognized Cybersecurity Practices
- Health Industry Cybersecurity Practices 2023 (Joint
- Cybersecurity for Clinician Video Training Series
- Health Industry NIST CSF Implementation Guide (Joint)
- Managing Legacy Technology Security
- Artificial Intelligence Machine Learning

2022

- Operational Continuity-Cyber Incident Checklist

2022

- MedTech Vulnerability Communications Toolkit
- Model Contract-Language for Medtech Cybersecurity

2021

- Securing Telehealth and Telemedicine

2020

- Supply Chain Risk Management
- Health Sector Return-to-Work Guidance
- Tactical Crisis Response
- Protection of Innovation Capital
- Information Sharing Best Practices
- Checklist for Teleworking Surge During COVID-19

2019

- Matrix of Information Sharing Organizations
- Workforce Guide
- Medical Device and Health IT Joint Security Plan
- Health Industry Cybersecurity Practices

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cybersecurity for the Clinician Video Training Series

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Sector Cybersecurity Five-Year Strategic Plan

Five years after the publication of the 2017 HHS-Health Care Industry Cybersecurity Task Force report found healthcare cybersecurity to be in "critical condition":

- Identify the HCIC recommendations that the HSCC Cybersecurity Working Group publications have addressed, and which remain a priority for CWG and sector attention;
- Assess how identified healthcare industry trends over the next five years may present continued or emerging cybersecurity challenges to the sector;
- Recommend how the industry and government should prepare for those changes, with a measurable vision of what "Stable Condition" looks like in 2029; and
- Prescribe specific initiatives and tactics that the CWG and government must do as a public-private partnership to motivate and facilitate the achievement of those preparedness objectives.

Questions

California Hospital Association

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Contact

Lisa Bisterfeldt
Cyber Resiliency Program Manager
HSCC OCCI Task Group Co-Author
St. Luke's Health System
bisterfl@slhs.org

HSCC LinkedIn Page

Greg Garcia
Executive Director
Health Sector Coordaining Council
Greg.Garcia@HealthSectorCouncil.org

Get Involved

HSCC Website Link