# Healthcare & Public Health Sector Coordinating Council

## *Cybersecurity Working Group*

## 2024 First Half Report

*Approved for public release*

Health Sector Coordinating Council
Cybersecurity Working Group

# Chairman's Forward

**Erik Decker**
**Industry Co-Chair**
**HSCC Cybersecurity Working Group**

This report comes to you as a first-half 2024 summary versus our normal quarterly report. The velocity and linkage of developments throughout the first half suggested we consolidate our report to provide the HSCC CWG membership a coherent perspective on our activities and related policy actions.

## On Our Heels to Leaning Forward

Clearly a major catalyzing event in 2024 was the Change Healthcare ransomware attack, which occurred one week before we launched the Health Industry Cybersecurity Strategic Plan (HICSP) in February after 18 months of development. The timing of the two events, along with the following Ascension incident, put an exclamation point on how the sector's defensive posture against the unrelenting pace of cyber incidents must be both reflexive and forward-looking to anticipate evolving threats. While we cannot say that a broad cross-section of the industry was prepared for the cascading impact of *Change*, these colliding dynamics have accelerated an evolved level of awareness, organization and motivation across the sector to continue developing effective prescriptions for a cybersecurity wellness plan.

In sequence with these events was the government's release of the HHS Cyber Performance Goals (CPGs), the HHS one-stop shop "Cyber Gateway" and the White House National Security Memorandum-22. which together can set a floor for cybersecurity accountability, consolidate information resources for the sector, and accelerate our collective effort with government to identify, assess and manage sector wide risks. And it is expected that the CPGs may soon have regulatory leverage behind them to add operational and resource urgency. Toward that end, the CWG has been in regular consultations with our government partners to consider a phased approach to any new mandates that can combine accountability with flexibility and government support for the underserved.

## First Half Tees Up the Second

So peruse this report, particularly slides 7 & 8, which summarizes our ongoing momentum from what we have accomplished toward what remains for this year:

- 3 publications in the first and at least 4 more by the end of the year
- Broad visibility in conferences, webinars and podcasts across the country, plus testimony at a Congressional hearing and a redesigned website
- Two new task groups launched in Q1 and a soon-to-be formed joint task group with HHS on AI Cybersecurity
- 32 new member organizations joined
- Coming establishment of a comprehensive HICSP implementation plan task group
- First-ever All-Hands Across America hosted in 8 locations and the next All-Hands meeting November 19-20 in San Diego

***I assure you as we dash to the home plate in 2024 the momentum will pick up even more*** as we mobilize sector adoption and implementation of our many resources and the Strategic Plan and engage with our government to profile and mitigate the clinical, operational, financial, and supply chain risks across our sector. We know that the need for cybersecurity in healthcare is never waning so we will continue to rally behind the mobilizing words of the former National Cyber Director, Chris Inglis. We must organize our healthcare system such that **"*they have to beat all of us to beat one of us*"**.

# Membership

# CWG Membership

***From January 1 to June 30, 2024, an increase of 32 industry members to:***

- 438 organizational Industry members, including:
  - 53 Industry association members
  - 63 non-voting Advisor companies
- Government organizations include 11 federal agencies, 5 state agencies, 2 city agencies, and 2 Canadian
- Total representing personnel: 1036

# Subsector Distribution

- Direct Patient Care: **42.76%**
- Health Information Technology: **6.46%**
- Health Plans and Payers: **5.12%**
- Mass fatality and Management Services: **0**
- Medical Materials: **9.13%**
- Laboratories, Blood, Pharmaceuticals: **5.79%**
- Public Health: **4.68%**
- Cross-sector: **7.57%**
- Government (Fed, State, County, Local): **4.45%**
- Advisors: **14.03%**

# Priority Activities and Deliverables

Health Sector Coordinating Council
Cybersecurity Working Group

# Activities Highlights

## Publications

- Health Industry Cybersecurity Strategic Plan
- Coordinated Privacy Security Partnerships
- Medical Device and Health IT Joint Security Plan v2 (JSP2)

## New Task Groups

- Cybersecurity Updates and Patching
- Underserved Provider Cybersecurity Advisory Group

## Government Consultations

- Kick-off HHS NSM-22 “RAMP” Initiative (Risk Assessment and Management Program)
- April HSCC Testimony to House Energy and Commerce Committee
- Substantive input to HHS Cyber Performance Goals
- January 29 Briefing for White House on HSCC Cybersecurity Strategic Plan

## HSCC Visibility

- Website redesign and launch with HIC-SP publication
- 26 HSCC speaking engagements for executive director (more from leadership and members), including: conference keynotes and panels, podcasts, webinars, and press interviews

## Membership

- Increase of 32 industry members to 438
- 69 Orientation calls
- First-ever All-Hands Across America – 8 simultaneous locations in 1 day

# 2nd Half Priorities

1) Mobilize and Implement Five-Year Cybersecurity Strategic Plan
2) Work with HHS on NSM-22 Sector Mapping, Risk Assessment and Management Plan
3) Establish A.I. Cybersecurity Task Group with HHS
4) Publications before Y/E 2024:
   - ***Operational Manufacturing Technology Cybersecurity***
   - ***Model Contract v2***
   - ***Executive Checklist for Incident Response***
   - ***(Joint HHS-HSCC) Operational Continuity-Cyber Incident***
   - ***Medtech Vulnerability Communications***
5) Continue Task Group Work Streams for Cybersecurity Best Practices and Policy Recommendations
6) Support transition of HHS/HSCC 405(d) Partnership from HHS CIO to HHS ASPR
7) Promote Membership Integration between CWG and non-cyber HPHSCC Working Groups
8) November 19-20 All-Hands Membership Meeting
9) Cybersecurity Working Group Leadership elections for 2025

Health Sector Coordinating Council
Cybersecurity Working Group

# Q2 2024 Public Foot-Print

## All Publications

- Total downloads to-date: **151,400+**
- Video Training: **39,000+ views**

## Webpage Views

- Total Page Views: 31,408
- Total Users:  13,103

## Public Recognition

- 11 Press Mentions and Features
- 15+ Leadership Speaking Engagements

## LinkedIn Followers (since account opening October 2018)

- LinkedIn:  2,000

# Supplementary Background Material

Health Sector Coordinating Council
Cybersecurity Working Group

# HSCC CWG Publications

## *151,400 Downloads Since 2019*

https://healthsectorcouncil.org/hscc-publications

### 2024

- Medical Device and Health IT Joint Security Plan v2 (JSP2)
- Health Industry Cybersecurity Strategic Plan
- Coordinated Privacy Security Partnerships

### 2023

- *Updated* Health Industry Cybersecurity Information Sharing Best Practices
- *Updated* Health Industry Cybersecurity Matrix of Information Sharing Organizations
- 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
- 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 (Joint)

Health Sector Coordinating Council
Cybersecurity Working Group

# Task Groups
# Objectives And Leadership

| TASK GROUP | OBJECTIVE / DELIVERABLE | INDUSTRY LEADS | GOVT. LEADS |
|---|---|---|---|
| **405d – (Health Industry Cyber Practices)** | (Joint HHS-SCC publication) - Joint Industry/HHS Task Group (from §405(d) of the Cybersecurity Act of 2015) created the HICP (Health Industry Cybersecurity Practices) and is developing supporting collateral material and timely cyber events, marketing and partnerships. Version 2 published Spring 2023. See: https://405d.hhs.gov/ | Intermountain Health | HHS OCIO |
| **Incident Response Business Continuity** | Published Operational Continuity Cyber Incident (OCCI) April 2022 – toolkit for health provider operations during extended outage following ransomware attack. Follow-on publication Q2 2023 on Coordinated Healthcare Incident Response Plan (CHIRP) for cyber incident response and business continuity plan aligned with existing physical incident response protocols. Third initiative in development – Executive/CEO questions-decision checklist for incident response. | St. Lukes Health<br>Duke Health<br>University of Vermont Health<br>Coastal Bend Regional Advisory Council | HHS HC3 |
| **Medical Technology Updating and Patching** | Develop a guide for mutual expectations among health delivery organizations and medical device manufacturers about updating and patching medical devices in the clinical environment, and associated risk, prioritization and cost. | Velentium<br>Health ISAC | HHS FDA |
| **Medical Technology Vulnerability Communications** | Provide guidance to MDMs & HDO's for preparing, receiving and acting on medical device vulnerabilities. First publication April 2022 on patient awareness. Second version on HDO/MDM engagement and implementation in process. | Cleveland Clinic<br>Abbott<br>Medcrypt (Advisor) | HHS FDA |

Health Sector Coordinating Council
Cybersecurity Working Group

# Task Groups
# Objectives And Leadership (*cont'd)*

| TASK GROUP | OBJECTIVE / DELIVERABLE | INDUSTRY LEADS | GOVT. LEADS |
|---|---|---|---|
| **Manufacturing Operational Technology** | Developing leading practices for cybersecurity management of operational/manufacturing technology. Initially focused on medical technology and pharmaceutical subsectors. | Becton Dickinson<br>Merck | HHS FDA |
| **Outreach and Awareness** | Develop CWG brand and document formatting templates, and marketing strategy for publications and messaging | Abbott<br>Censinet (Advisor) | HHS HC3 |
| **Public Health Cybersecurity** | Identify strategies for strengthening the cybersecurity and resilience of SLTT public health agencies with the support of private sector and academic organizations. | The UT Austin | HHS ASPR |
| **Risk Assessment** | (Joint HHS-SCC publication) - Joint publication with HHS April 2023 on NIST Cyber Framework Implementation guide. New initiative to develop guidance for aligning health enterprise controls with NIST CSF implementation tiers | HITRUST | HHS FDA |
| **Underserved Provider Cybersecurity Advisory Group** | Conduct a series of documented panel discussions with management of under-resourced providers to interview for perspectives about cybersecurity challenges, financial and operational challenges, and their needs for assistance to meet cybersecurity obligations | OCHIN, Inc.<br>Lakewood Health System | DHS CISA |

Health Sector Coordinating Council
Cybersecurity Working Group

# Cybersecurity Working Group
# 2024 Industry Executive Committee

**CHAIR**: Erik Decker, VP, CISO, Intermountain Healthcare

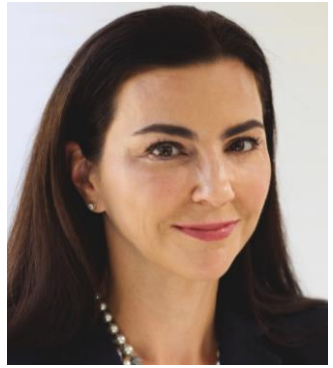
**VICE CHAIR**: Chris Tyberg, CISO, Abbott

**AT-LARGE:** Sanjeev Sah, CISO, Novant Healthcare

**CROSS SECTOR**: Bobby Rao, Global CISO, Esper Group

**DIRECT PATIENT CARE**: Julian Goldman, MD, Medical Director, Biomedical Engineering Mass General Brigham

**DIRECT PATIENT CARE**: Samantha Jacques, VP Corporate Clinical Engineering, McLaren Healthcare



**HEALTH IT**: Jennifer Stoll, Executive Vice President External Affairs, OCHIN, Inc.

**MEDICAL TECHNOLOGY:** Chris Reed, VP Product Security, Medtronic

**PLANS-PAYER**: Adrian M. Mayers, Dr.BA, VP & CISO, Premera Blue Cross

**PHARMA-LAB-BLOOD**: Janet Scott, VP, Business Technology Risk Management and CISO, Organon

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

**HEALTH-ISAC OPERATIONAL LIAISON *(non-voting)*:** Denise Anderson, President and CEO, Health-ISAC

# JCWG Government Co-Chairs

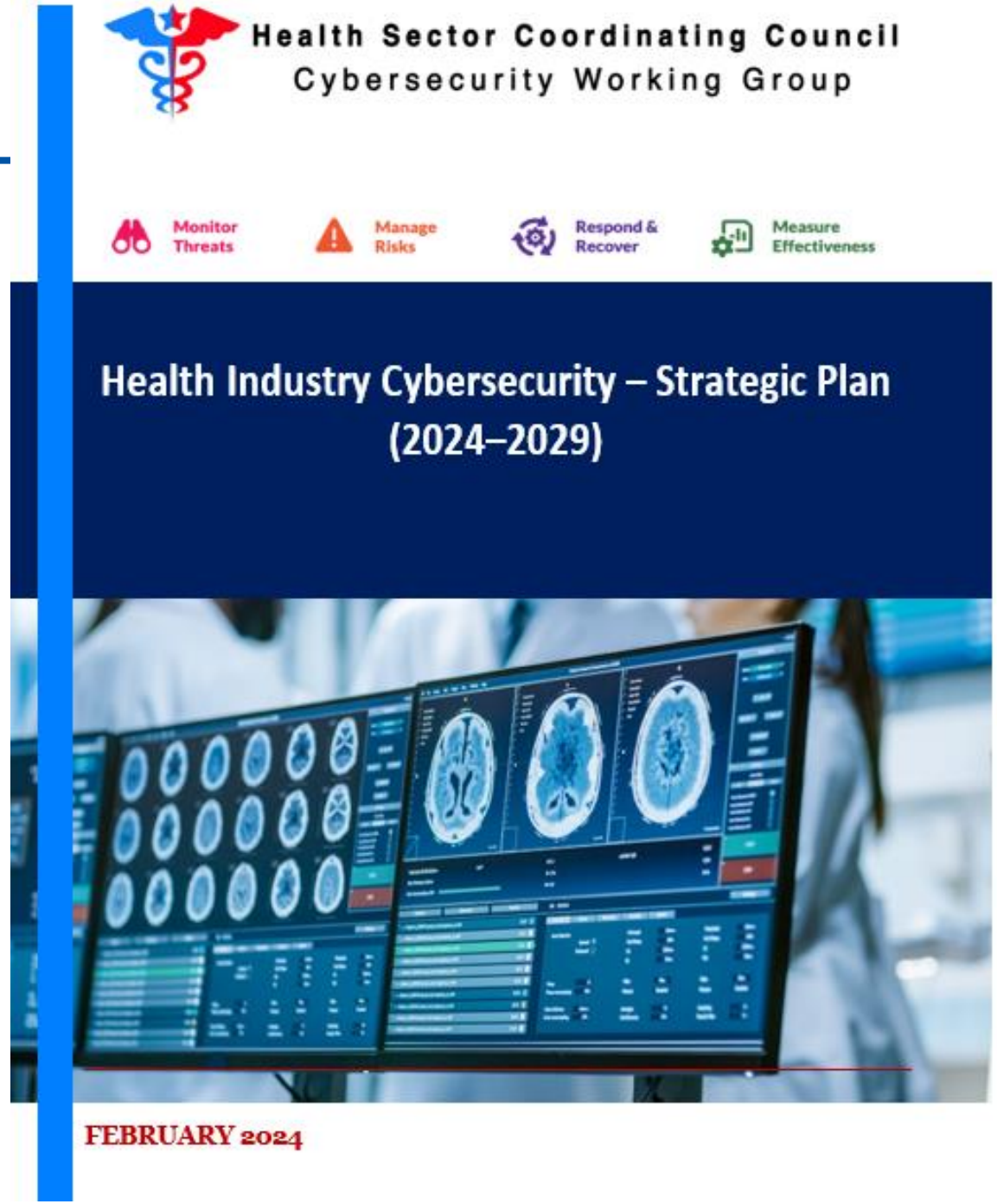
**Brian Mazanec**
Deputy Assistant Secretary and Deputy Director
Center for Preparedness
Administration for Strategic Preparedness and Response

**Suzanne Schwartz**
Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health
U.S. Food and Drug Administration

**Julie Chua**
Director, GRC Division
HHS Office of the Chief Information Officer

# Health Industry Cybersecurity Strategic Plan HICSP

# Five-Year Health Industry Cybersecurity Strategic Plan (HIC-SP)



# Health Industry Trends 2024-29

**Seven business, technology, clinical, and policy trends will characterize the evolution of the health sector over the next five years and beyond.**

**Trend 1:** **Methods of care delivery** will continue to shift and evolve

**Trend 2:** Adoption of **emerging and disruptive technologies** will accelerate

**Trend 3:** The **business of healthcare** will continue to change and adapt

**Trend 4:** **Acute Financial Distress** will not abate

**Trend 5:** **Workforce recruitment and talent** management will face competitive supply and demand pressures

**Trend 6:** Government will be challenged to **develop balanced policy that achieves objectives in complex health systems**

**Trend 7:** **Global instability, climate change and downstream effects** will increase pressure on the healthcare supply chain

Health Sector Coordinating Council
Cybersecurity Working Group

# Five-Year Cybersecurity Goals to Address Industry Trends

| | | | |
|---|---|---|---|
| G1 | Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant | G6 | Healthcare technology used inside and outside of the organizational boundaries is secure-by-design and secure-by-default while reducing the burden and cost on technology users to maintain an effective security posture |
| G2 | Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners | G7 | A trusted healthcare delivery ecosystem is sustained with active partnership and representation between critical and significant technology partners and suppliers, including non-traditional health and life science entities |
| G3 | Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors | G8 | Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing |
| G4 | Health, commercially sensitive research, and intellectual property data are reliable and accurate, protected, and private while supporting interoperability requirements | G9 | The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services |
| G5 | Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use | G10 | Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels within each organization |

Health Sector Coordinating Council
Cybersecurity Working Group

# Five-year Cybersecurity Objectives to Implement the Goals

| | | | |
|---|---|---|---|
| O1 | Develop, adopt and demand safety and resilience requirements for products and services offered, from business to business, as well as health systems to patients, with the concept of secure-by-design and secure-by-default | O7 | Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs |
| O2 | Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data | O8 | Increase utilization of automation and emerging technologies like AI to drive efficiencies in cybersecurity processes |
| O3 | Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system | O9 | Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements |
| O4 | Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies | O10 | Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks |
| O5 | Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations | O11 | Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness |
| O6 | Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health) | O12 | Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurity incidents |

# 2029 Target Future State

**If we succeed, our healthcare cybersecurity diagnosis will upgrade from "Critical Condition" in 2017 to "Stable Condition" in 2029. HIC-SP will lead us to an end-state environment in which cybersecurity is ingrained as a public health and patient safety standard:**






| Reflexive Cybersecurity | Secure Design & Implementation | C-Suite Ownership | Cyber Safety Net | Cyber Competence | 911 Cyber Civil Defense |
|---|---|---|---|---|---|
| Both practiced and regulated healthcare cybersecurity is reflexive, evolving, accessible, documented and implemented for practitioners and patients. | Technology and services across the healthcare ecosystem is a shared and collaborative responsibility. | Healthcare C-Suite embraces accountability for cybersecurity as enterprise risk and a technology imperative. | Under-resourced health organizations are supported in the form of financial, policy and technical assistance ensuring cyber equity across the ecosystem. | Workforce learning and application is an infrastructure wellness continuum. | Ensures that early warning, incident response and recovery are reflexive, collaborative and always on. |

**Greg Garcia**
**Executive Director**
Greg.Garcia@HealthSectorCouncil.org

**Allison Burke**
**Member Engagement Project Manager**
Allison.Burke@HealthSectorCouncil.org

*For more information, visit https://HealthSectorCouncil.org*