# On the Edge: Cybersecurity Health of America's Resource-Constrained Health Providers

Health Sector Coordinating Council
Cybersecurity Working Group

May 2025

# Underserved Provider Cybersecurity Initiative

# Agenda

DETAILS OF INTERVIEWS

GENERAL FINDINGS FROM INTERVIEWS

RECOMMENDATIONS – FOLLOW UP

# Resource-Constrained Definition

## Defined For This Project

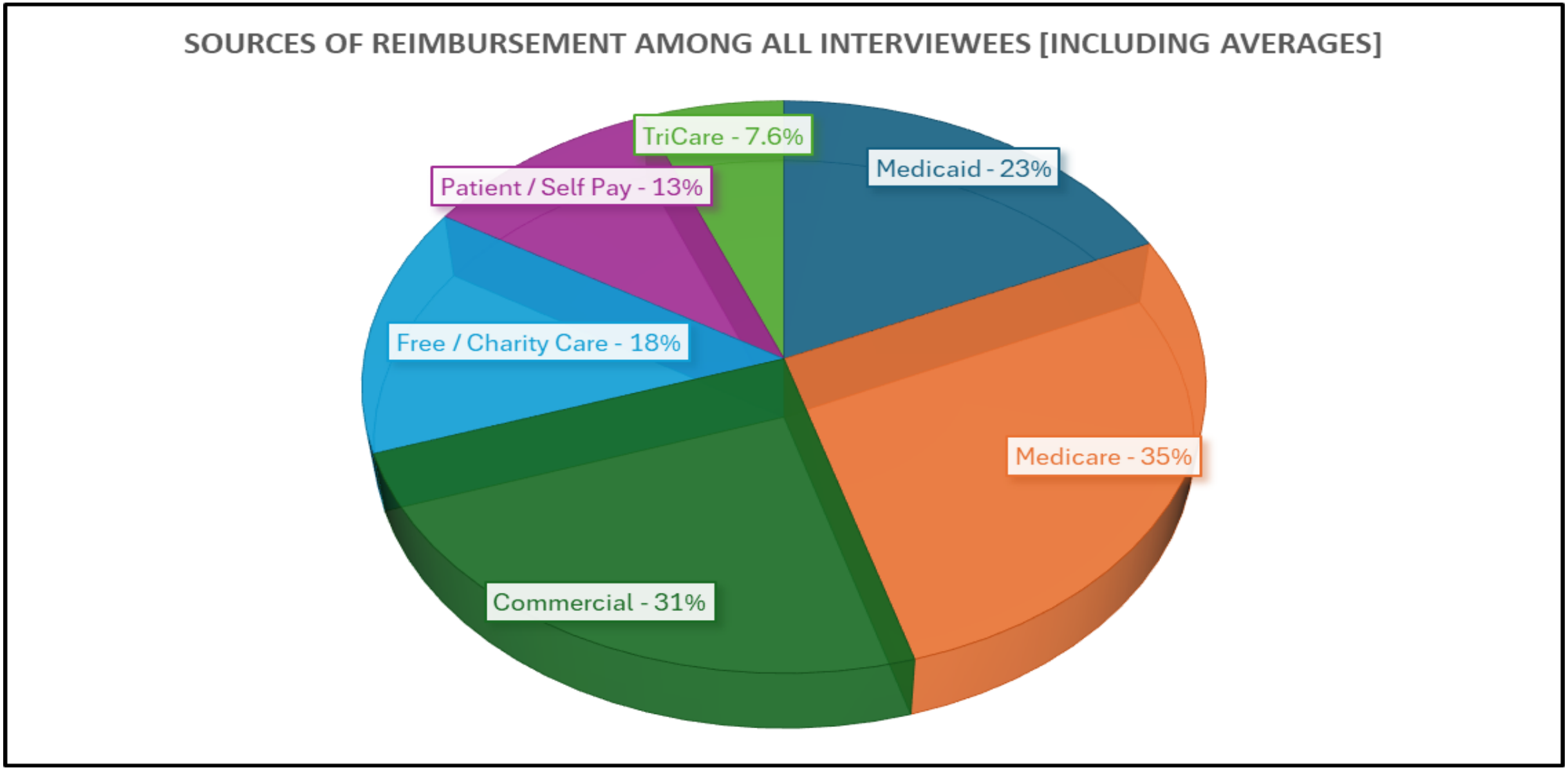
A medical facility or individual practitioner encountering significant obstacles in providing comprehensive healthcare services and conforming to operation standards, often due to financial constraints, geographic isolation, or patient population characteristics. These constraints further impede the ability of Resource-Constrained health providers to implement, maintain, and enhance cybersecurity measures.

Health Sector Coordinating Council
Cybersecurity Working Group

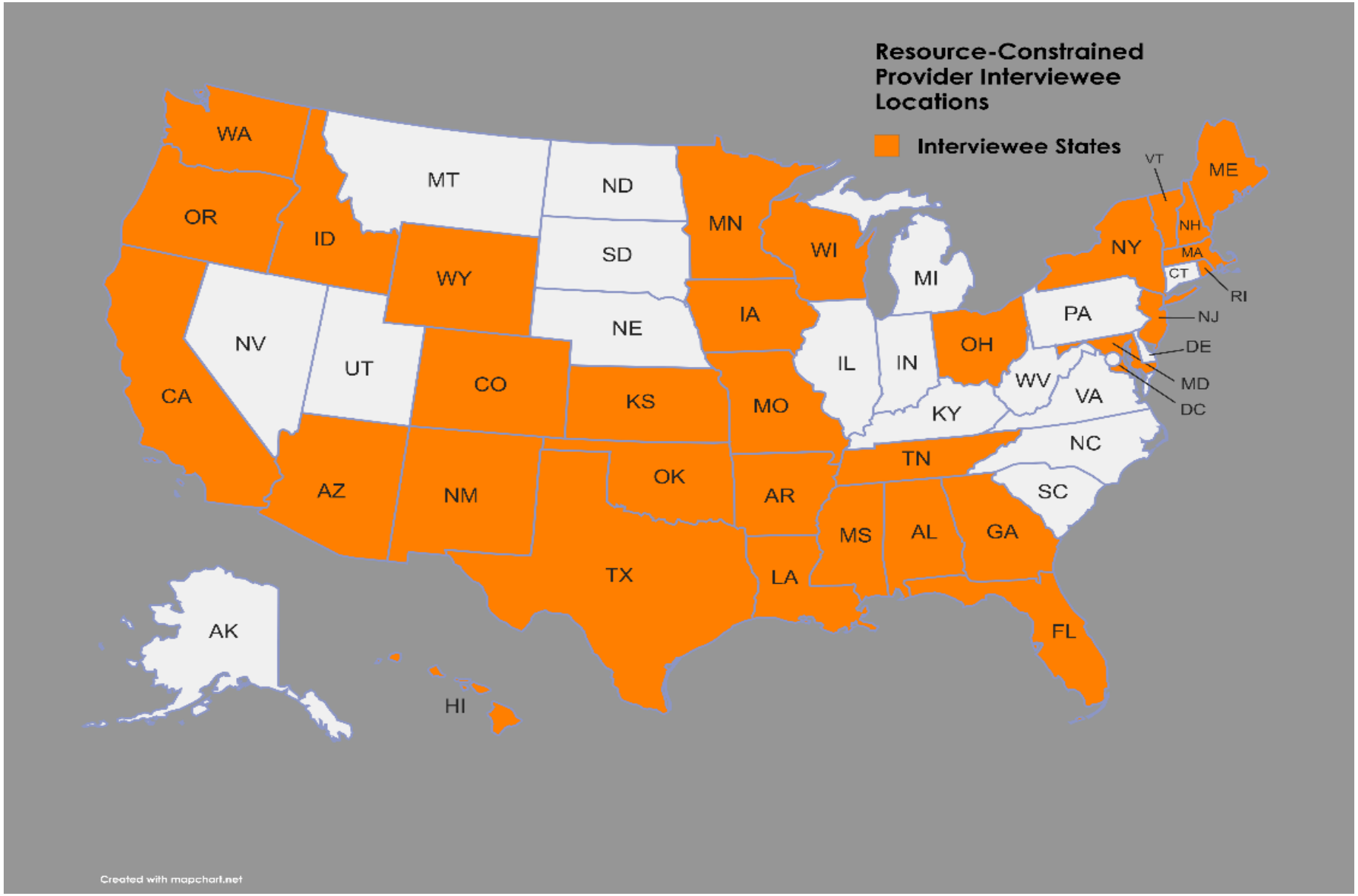
# Provider-Types Interviewed

- CAH (Critical Access Hospital)
- Disproportionate Medicare/Medicaid dependence
- FQHC (Federally Qualified Health Center)/ Look-Alike
- Free Clinic
- LTC (Long Term Care)
- Native American / Tribal / IHS (Indian Health Service)
- Regional Health System
- REH (Rural Emergency Hospital)
- RHC (Rural Health Clinic)
- SAMHSA (Substance Abuse and Mental Health Services Administration)
- Small Practice
- SNF (Skilled Nursing Facility)

# Revenue Sources



# Interviewee Locations



Health Sector Coordinating Council
Cybersecurity Working Group

# Cyber Health

## Resource Constrained Healthcare Providers

- Healthcare most affected by the highest volume of third-party breaches, followed by financial services.
- 14% of healthcare organizations say their IT security teams are fully staffed. Over half say they need more help, and 30% say they are understaffed or severely understaffed.

- Resource constrained healthcare providers report antiquated systems, multiple points of vulnerability and inability to adopt new cyber technologies (MFA).
- Lack staff and myriad of standards (state and federal) increase cost and complexity.

- Drive adoption of modernized health IT
- Prioritize new models of upskilling and workforce development and training
- Drive efficiencies and economies of scale for monitoring, technical assistance, and threat response leveraging provider networks

---

Cyber Attacks Dramatically Increasing

Resource Constrained Impact Ecosystem

Recommendations Cyber Health

Health Sector Coordinating Council
Cybersecurity Working Group

# Recommendations

**Third Party Vendors & Risk Management**

**Not Solely Health Provider Responsibility**

**Workforce Augmentation for Cybersecurity**

**Funded At Federal & State Level**

**CMS Reimbursement Hesitancy If Tied To Compliance**

**USDA Rural Loan Program**

**Continuation & Expansion**

**Training & Best Practice Library**

**Regulatory & Technical**

Health Sector Coordinating Council
Cybersecurity Working Group

# Under Served Provider Cybersecurity Task Group Chairs

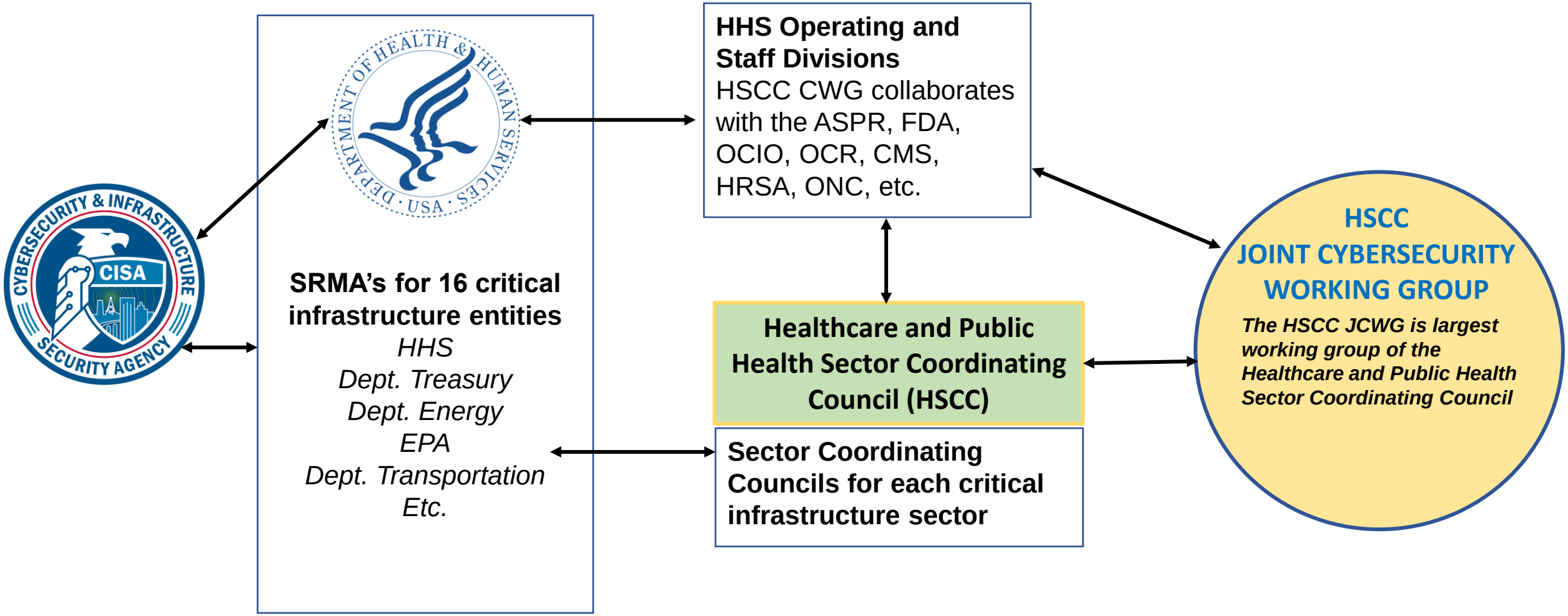
**Jennifer Stoll**
**Chief External Affairs Officer**
**OCHIN**

**Jim Roeder**
**Vice President of IT**
**HIPAA Security & Privacy Officer**
**Lakewood Health System**

# Health Sector Coordinating Council Cybersecurity Working Group

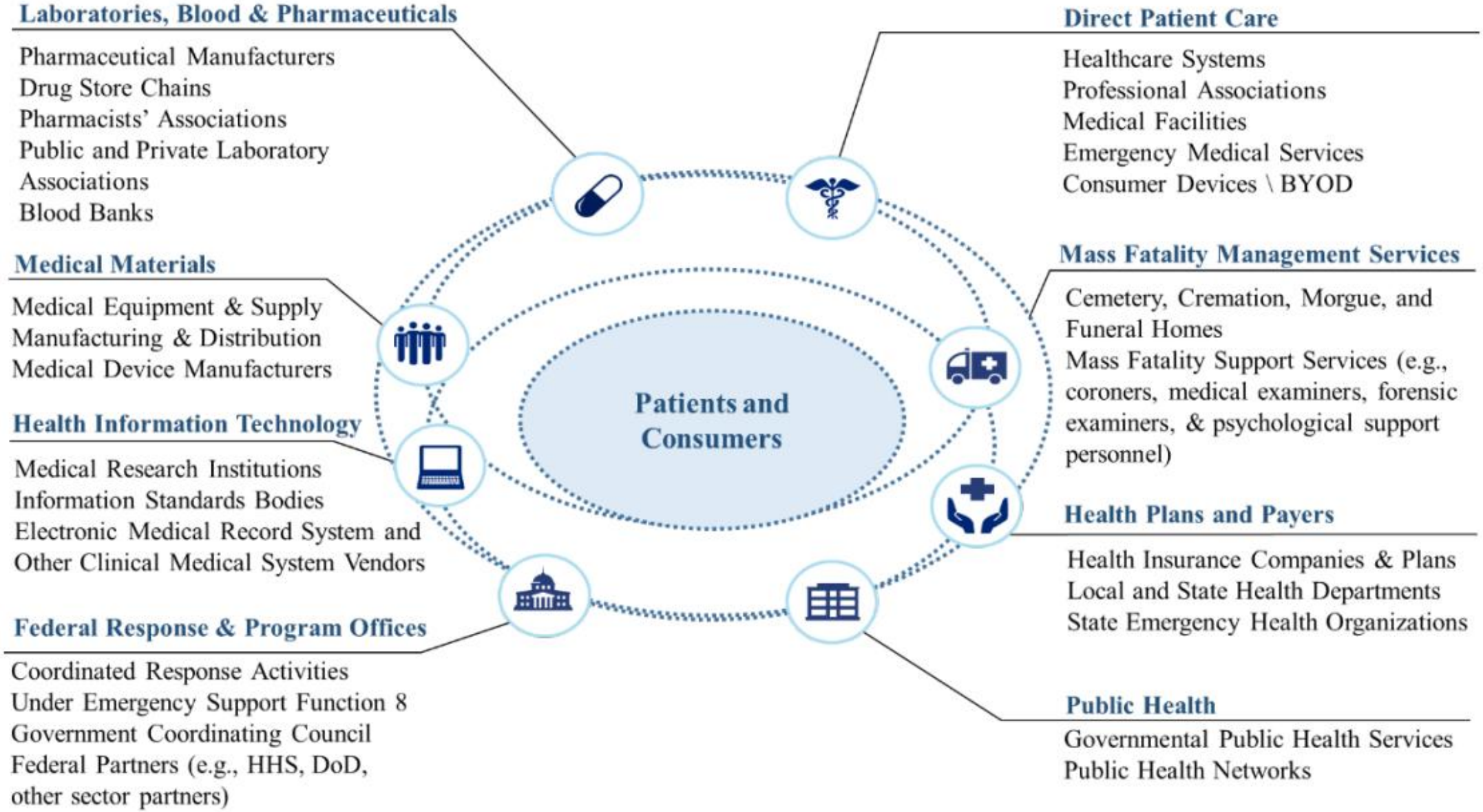
Health Sector Coordinating Council
Cybersecurity Working Group

# Critical Infrastructure Protection Public Private Partnership



Health Sector Coordinating Council
Cybersecurity Working Group

# The Health Sector - An Interconnected Ecosystem



# HSCC Joint Cybersecurity Working Group (CWG)

## Mission

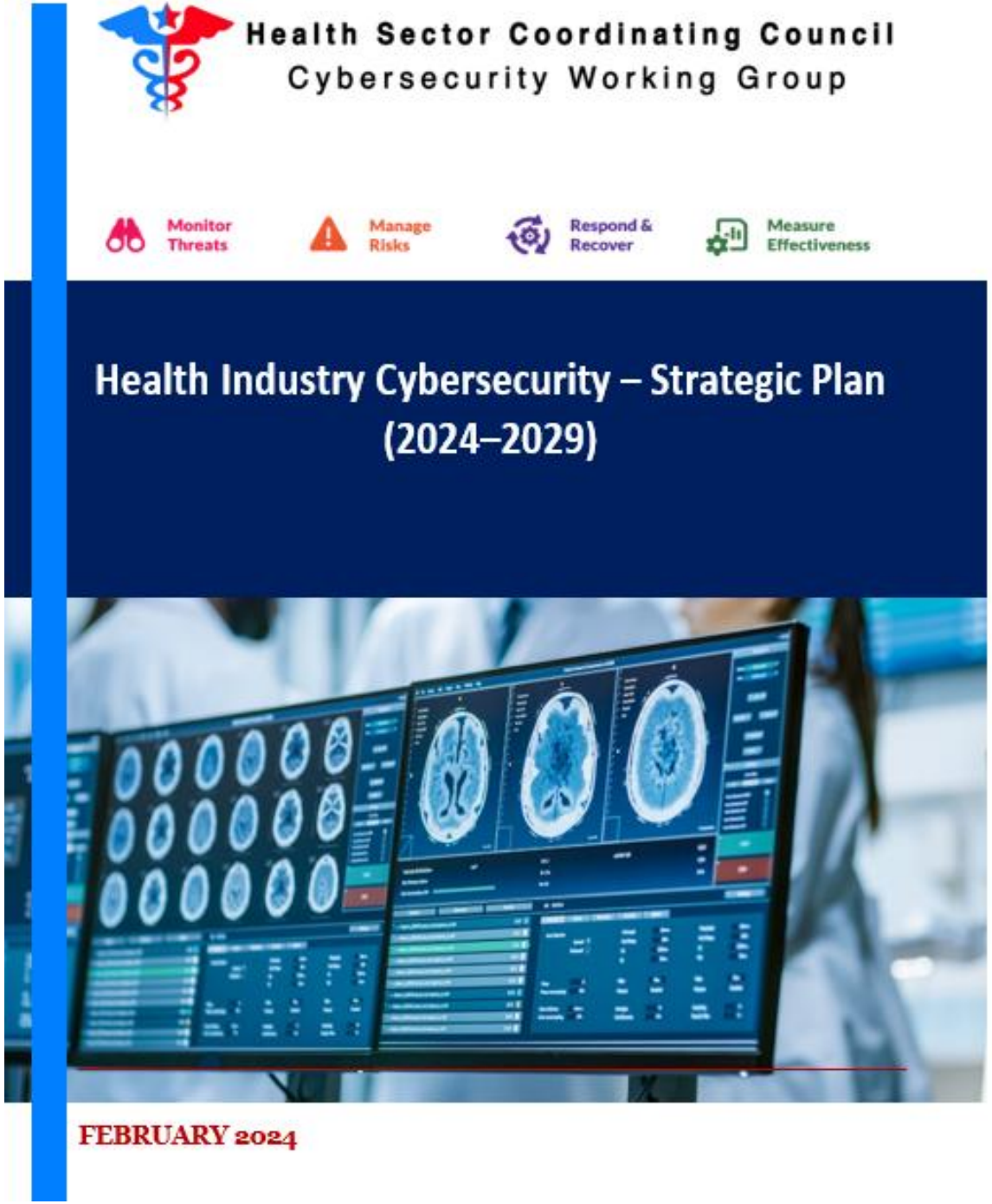
- Industry advisory council that identifies and develops strategic, cross-sector solutions to cybersecurity threats and vulnerabilities affecting the security and resiliency of the healthcare sector
- Outcome-oriented task groups develop best practices; Full JCWG membership meets twice a year in-person around the country
- Works closely on joint initiatives with:
  - HHS Administration for Strategic Preparedness and Response
  - Food and Drug Administration
  - Other HHS Operating Divisions and DHS CISA

# HSCC Joint Cybersecurity Working Group (CWG)

## Membership

- Largest standing Working Group under the HSCC umbrella
  - **456 private sector organizations**, including:
    - 393 owner-operators
      - Includes 53 industry associations and professional societies
    - 63 non-voting advisor companies
  - **20 government organizations**, including 11 federal, 4 state, 2 city, 1 county and 2 Canadian
  - Total representing **personnel: 1036**

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



Health Sector Coordinating Council
Cybersecurity Working Group

# Cybersecurity Strategic Plan Implementing Objectives

| | | | |
|---|---|---|---|
| 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, the diagnosis of healthcare cybersecurity will upgrade from "Critical Condition" in 2017 to "Stable Condition" in 2029. "Cyber Safety is Patient Safety" will be characterized by:**

## Reflexive Cybersecurity

Both practiced and regulated healthcare cybersecurity is reflexive, evolving, accessible, documented and implemented for practitioners and patients.

## Secure Design & Implementation

Technology and services across the healthcare ecosystem is a shared and collaborative responsibility.

## C-Suite Ownership

Healthcare C-Suite embraces accountability for cybersecurity as enterprise risk and a technology imperative.

## Cyber Safety Net

Under-resourced health organizations are supported in the form of financial, policy and technical assistance ensuring cyber equity across the ecosystem.

## Cyber Competence

Workforce learning and application is an infrastructure wellness continuum.

## 911 Cyber Civil Defense

Ensures that early warning, incident response and recovery are reflexive, collaborative and always on.

Health Sector Coordinating Council
Cybersecurity Working Group

# Leading Practices
# By the Sector for the Sector

**2025**

- One the Edge : Cyber Health of Resource-Constrained
- Cybersecurity Consultative Process Proposal
- Recommendations for Government Policy and Programs

**2024**

- Medical Product Manufacturer Cyber Incident Response Playbook
- Executive Checklist for Incident Response
- Medical Device and Health IT Joint Security Plan v2 (JSP2)
- Health Industry Cybersecurity Strategic Plan
- Coordinated Privacy Security Partnerships

**2023**

- Health Industry Cybersecurity Information Sharing Best Practices
- Health Industry Cybersecurity Matrix of InfoSharing 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

**.... 2023**

- 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
- Checklist for Teleworking Surge  During COVID-19

**2019**

- Workforce Guide
- Medical Device and Health IT Joint Security Plan
- Health Industry Cybersecurity Practices (Joint)

***Link to publications***

# THANK YOU

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