Health Sector Coordinating Council
Cybersecurity Working Group

HEALTH INDUSTRY CYBERSECURITY STRATEGIC PLAN (HIC-SP) 2024-2029

CYBER PANDEMIC IN THE HEALTH SECTOR

ERROR 404

Patient Not Found

HEALTHCARE CYBERSECURITY
VITAL SIGNS IN CRITICAL CONDITION

- **HIPAA breaches in 2023 nearly doubled to 725 since 2018**

- **Ransomware Hit 141 Hospitals in 2023 – avg. ransom $1.5M, *Impacting*:**
  - **Imaging and other diagnostic and therapeutic devices**
  - **Loss of patient medical records**
  - **Down payment systems**
  - **Loss & corruption of clinical trial & research data**
  - **Pharmaceutical manufacturing operations**

"If you are unlucky enough to be in the hospital when a ransomware attack occurs, your risk of dying goes up"

Health Sector Coordinating Council
Cybersecurity Working Group

WHO IS THE NEXT HEADLINE

At Least 141 Were Hospitals Directly Affected by Ransomware Attacks in 2023

Study finds that "targeted hospital cyberattacks …associated with disruptions of health care delivery … should be considered a regional disaster."

Parents struggle to get care after cyberattack on Chicago children's hospital

Hospital systems have been affected for more than a week.

Health IT - Why This Matters

When hospital ransomware attacks target patients: A new trend to follow

FORBES › INNOVATION › CYBERSECURITY

Ransomware Attack Takes 100 Hospitals Offline

"If you are unlucky enough to be in the hospital when a ransomware attack occurs, your risk of dying goes up"

Health Industry Cybersecurity Strategic Plan 2024-29 (HIC-SP)

Objective

- Identify healthcare industry trends over the next five years
- Assess associated cybersecurity challenges
- Recommend cybersecurity strategy to upgrade from "Critical Condition" to "Stable Condition" in 2029; and
- All hands on deck – health providers, medtech and health IT, pharmaceutical, health plans and payers, and government: implement and facilitate achievement of the strategy.

Who is Prescribing the Wellness Plan

Health Sector Coordinating Council
Joint Cybersecurity Working Group

- Government-recognized critical infrastructure advisory council of more than 400 healthcare providers, life sciences, medtech, payers, health IT & public health entities
- Partners with government to identify and mitigate cyber threats to patient care, health data & research, IT & medical technology systems, manufacturing operations
- Publishes freely-available healthcare cybersecurity best practices and policy recommendations – by the sector for the sector
- Organizing imperative that ***Cyber Safety is Patient Safety***.

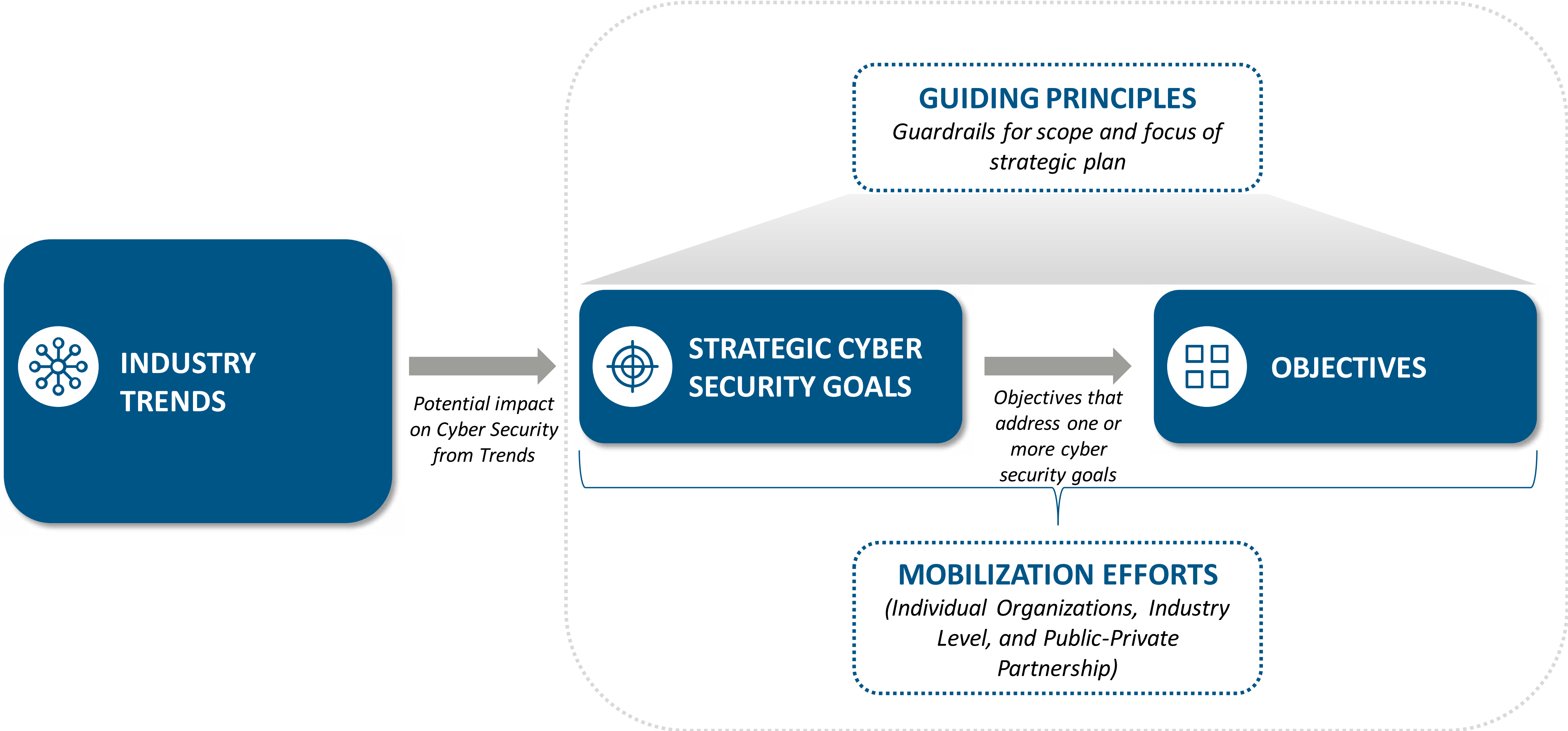
HIC-SP 2024-2029

- Co-Chaired by HSCC and HHS - 20 month process
- Forward looking & strategic
- Covers all industry sectors
- Audience: C-suite executives, Information Technology and Security leaders
- Plan with measurable outcomes across multiple subsector

The **Health Industry Cybersecurity Strategic Plan** puts patient safety in the center, while supporting innovation, resilience, and the move to the future of health.

Strategic Plan Structure

The following depicts the structure of the HIC-SP. Projected 5-year industry trends informed identification of broad cybersecurity goals realized by actionable implementing objectives to move the sector toward a more cyber-secure and resilient posture.



Five-Year Health Industry Trends

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

5-Year Cybersecurity Goals Meet Industry Trends

The health industry will pursue ten cybersecurity goals to meet the challenges posed by industry trends.

Goal 1

Healthcare and wellness delivery services are user-friendly, accessible, safe, secure, and compliant.

Goal 2

Cybersecurity and privacy practices and responsibilities are understandable to healthcare technology consumers and practitioners.

Goal 3

Cybersecurity requirements are readily available, harmonized, understandable, and feasible for implementation across all relevant healthcare and public health subsectors.

Goal 4

Health data, commercially sensitive research, and intellectual property data are reliable and accurate, protected and private, while supporting interoperability requirements.

Goal 5

Emerging technology is rapidly and routinely assessed for cybersecurity risk, and protected to ensure its safe, secure, and timely use.

Goal 6

Healthcare technology used inside and outside of organizational boundaries is secure-by-design and secure-by-default while reducing the cybersecurity burden and cost on technology users.

Goal 7

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.

Goal 8

Foundational resources and capabilities are available to support cybersecurity needs across all healthcare stakeholders regardless of size, location, and financial standing.

Goal 9

The health and public health sector has established and implemented preparedness response and resilience strategies to enable uninterrupted access to healthcare technology and services.

Goal 10

Organizations across the health sector have strong cybersecurity and privacy cultures that permeate down from the highest levels with-in each organization.

Cybersecurity Objectives
Implement 5-Year Goals

Enterprise and sector-wide implementation of twelve cybersecurity objectives will achieve the proposed cybersecurity goals that address the identified sector trends.

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 by-default.	**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.	**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.	**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.
O5. Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations.	**O6.** Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health).	**O7.** Increase incentives, development and promotion of healthcare cybersecurity-focused education and certification programs.	**O8.** Increase utilization of automation and emerging technologies such as AI to drive efficiencies in cybersecurity processes.
O9. Develop health subsector-specific integrated cybersecurity profiles aligned with regulatory requirements.	**O10.** Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks.	**O11.** Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness.	**O12.** Develop mechanisms to enable "mutual aid" support across sector stakeholders to allow for timely and effective response to cybersecurity incidents.

Health Sector Coordinating Council
Cybersecurity Working Group

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.

Health Sector Coordinating Council
Cybersecurity Working Group

Health Organizations Support Health Industry Cybersecurity Strategic Plan

The Undersigned Organizations agree:

- The United States Healthcare and Public Health (Health) Sector continues to face dramatic increases in cyber-attacks, causing disruption to patient safety, the care continuum and the operation of supporting network-connected products and services;
- Cyber preparedness and resiliency of the Health Sector depends on a collective defense involving all Health subsectors and supporting infrastructure in the interconnected and interdependent ecosystem;
- Progress has been made in awareness and implementation of Health Sector guidance for cybersecurity risk management, but efforts must be accelerated in an All-of-Sector, national collective strategy; and
- The Health Sector Coordinating Council Joint Cybersecurity Working Group has developed a Five-Year Health Industry Cybersecurity Strategic Plan (HIC-SP) that presents a wellness plan for lifting Health Sector cybersecurity from “critical condition” to “stable condition” by 2029.

The undersigned therefore embrace *the principles of the Health Industry Cybersecurity Strategic Plan to enhance our shared preparedness and resiliency on the imperative that “Cyber Safety is Patient Safety”*

HIC-SP Phase II

SIGN THE PLEDGE AND JOIN US

MOBILIZE & IMPLEMENT

DEFINE & TRACK MEASURES FOR SUCCESS

About the Health Sector Coordinating Council Joint Cybersecurity Working Group

Health Sector Coordinating Council
Cybersecurity Working Group

Interconnected Healthcare Ecosystem

Laboratories, Blood & Pharmaceuticals

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

Medical Materials

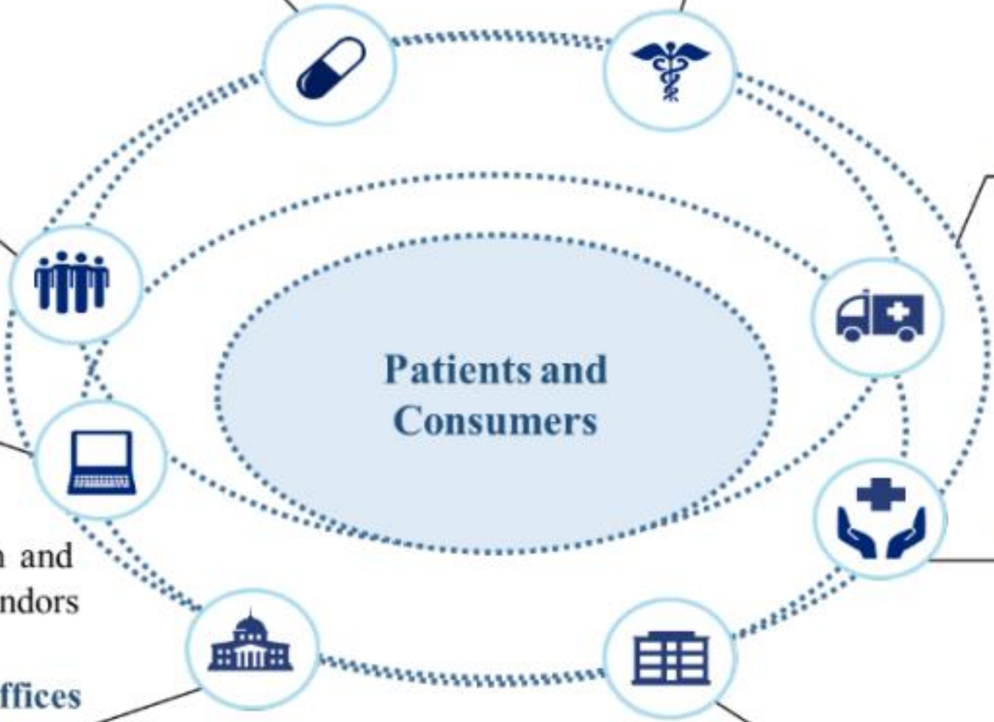
Medical Equipment & Supply Manufacturing & Distribution
Medical Device Manufacturers

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

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC Joint Cybersecurity Working Group (JCWG)

- Organized in 2018
  - **425 private-sector member organizations** (as of February 2024, ***600% increase since 2018***), including:
    - 52 industry associations
    - 58 non-voting Advisor firms
  - 19 Government organizations, including federal state, city and county
  - Total representing personnel: 980
- 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 through 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

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC JCWG Member Organization Distribution by Subsector

- Direct Patient Care: **40.5%**
- Health Information Technology: **6.8%**
- Health Plans and Payers: **5.3%**
- Mass fatality and Management Services: **0**
- Medical Materials: **9.6%**
- Laboratories, Blood, Pharmaceuticals: **6.0%**
- Public Health: **5.5%**
- Cross-sector: **8.2%**
- Government (Fed, State, County, Local): **3.9%**
- Advisors: **14.2%**

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC Publications Supplementing HIC-SP
By the Sector for the Sector

2024

- 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)

https://healthsectorcouncil.org/hscc-publications

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC Cybersecurity Working Group 2024 Industry Executive Committee

CHAIR: Erik Decker, VP, CISO, Intermountain Healthcare

VICE CHAIR: Chris Tyberg, CISO, Abbott

AT-LARGE: Sanjeev Sah, Vice President, CSO, CommonSpirit Healthcare

CROSS SECTOR: Bobby Rao, Global CISO, Fresenius Medical Care

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 Sector Coordinating Council
Cybersecurity Working Group

HSCC JCWG
Government Co-Chairs

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

Bob Bastani
Senior Cyber Security Advisor
Security, Intel, and Information Management Division
Administration for Strategic Preparedness and Response
U.S. Department of Health and Human Services

HEALTH SECTOR COORDINATING COUNCIL
Cybersecurity Working Group

Greg Garcia
Executive Director
Greg.Garcia@HealthSectorCouncil.org

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

Morgan Shuey
Member Support Intern
Morgan.Shuey@HealthSectorCouncil.org

https://HealthSectorCouncil.org