Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Coordinating Council Joint Cybersecurity Working Group

Cybersecurity Primer for Massachusetts Healthcare Providers

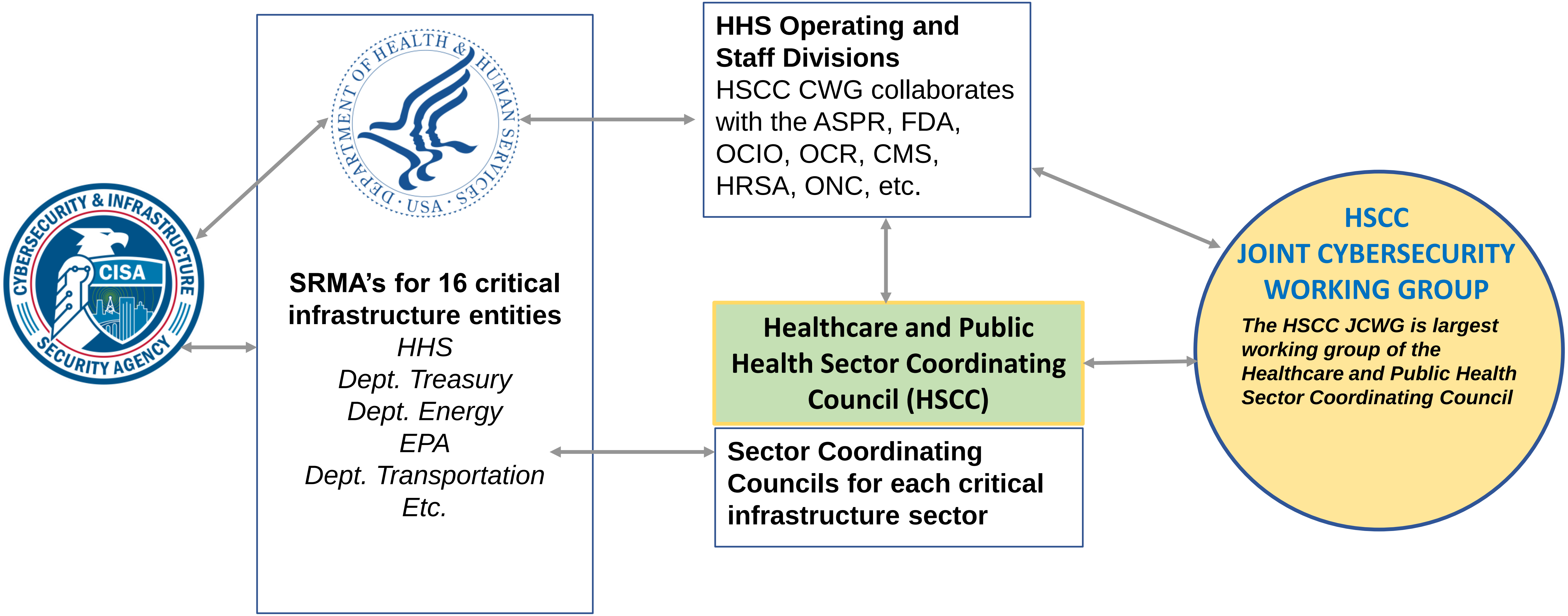
November 14, 2024

Greg Garcia
HSCC Cybersecurity Working Group Executive Director
greg.garcia@HealthSectorCouncil.org
https://HealthSectorCouncil.org

Critical Infrastructure Protection Policy Foundation

- National Security Memorandum 22 - Updates PPD 21 (below) to require enhanced coordination between sector risk management agencies and their industry sector partners for assessing and managing critical sector risk.
- E.O. 14028 - Improving the Nation's Cybersecurity - 2021
- P.L. 116-321 HITECH Act Amendment - Directs HHS Office for Civil Rights when enforcing a HIPAA breach to consider whether the victim entity has implemented the HHS-HSCC Health Industry Cybersecurity Practices (HICP), NIST Cybersecurity Framework, or other recognized cybersecurity practices as a potential basis for mitigating fines or favorably terminating an audit. - 2021
- National Defense Authorization Act, FY '21 (§9002, p. 1382) - Specifying partnership responsibilities of Sector Risk Management Agencies - 2020
- E.O. 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure –2017 – Transparency of critical sector threats (reporting), Electric sector, Botnets
- §405(d) Cybersecurity Act 2015 - Established a program under HHS to work with the health sector to develop cybersecurity best practices and guidelines - 2015
- E.O. 13691 – Promoting Private Sector Cybersecurity Information Sharing – 2015 ; Encouraging establishment of ISAOs
- E.O. 13636 (PPD-21) - Improving Critical Infrastructure Cybersecurity (resulted in the NIST Cybersecurity Framework)- 2013
- Foundational Presidential Executive Orders on Critical Infrastructure Protection and the public-private partnership (PDD-63 - 1998, and HSPD-7 - 2003)

Critical Infrastructure Protection Public Private Partnership


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

SRMA's for 16 critical infrastructure entities
HHS
Dept. Treasury
Dept. Energy
EPA
Dept. Transportation
Etc.

HHS Operating and Staff Divisions
HSCC CWG collaborates with the ASPR, FDA, OCIO, OCR, CMS, HRSA, ONC, etc.

Healthcare and Public Health Sector Coordinating Council (HSCC)

Sector Coordinating Councils for each critical infrastructure sector

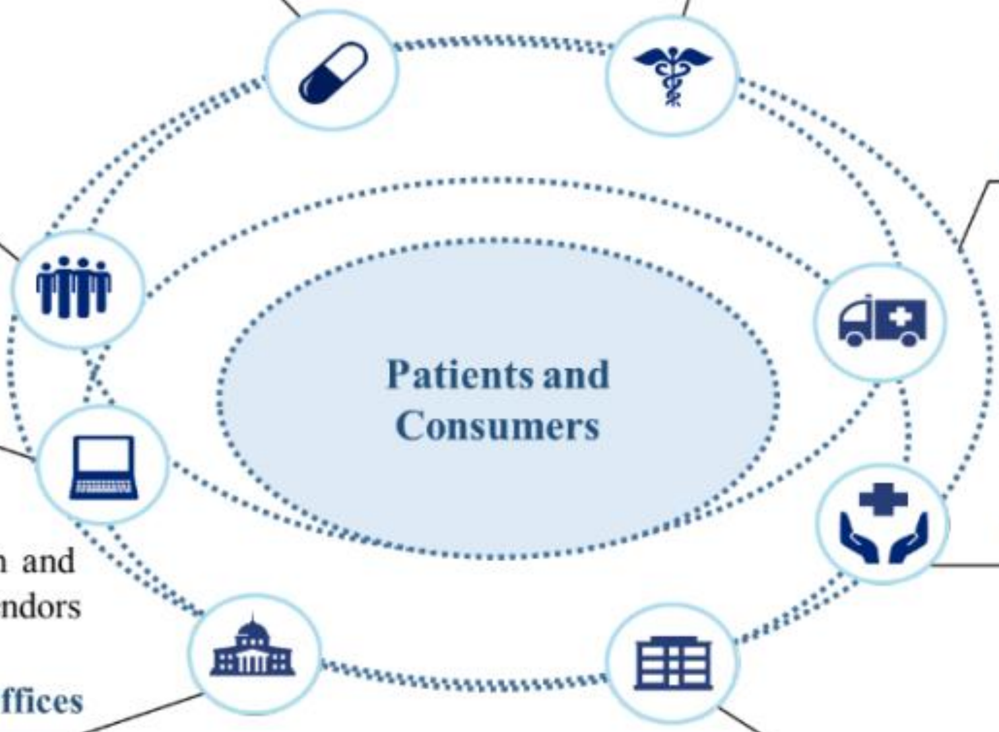
HSCC JOINT CYBERSECURITY WORKING GROUP

The HSCC JCWG is largest working group of the Healthcare and Public Health Sector Coordinating Council

Healthcare and Public Health Sector Coordinating Council

- 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

The Health Sector - An Interconnected 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 Joint Cybersecurity Working Group

HSCC Joint Cybersecurity Working Group (JCWG)

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

Membership

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

HSCC JCWG Member Distribution by Subsector

- 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%**

Membership Eligibility and Expectations

Voting “Owner-Operator” Members

- Covered Entities and Business Associates involved in direct patient care subject to HIPAA
- Health plans and payers
- Medical materials, technology, and distribution subject to FDA regulation
- Pharmaceuticals, laboratories, blood entities subject to FDA regulation
- Health Information Technology owners, operators and manufacturers subject to interoperability rules
- Mass fatality management services
- Trade groups and professional societies representing any of the above
- Government (state, local, tribal, territorial, and federal)

Voting Members elect the CWG Executive Committee (which elects Chair and Vice Chair) and vote as requested on approval of publications and any other CWG decisions and positions

Non-Voting Advisor Members

- Entities that are not regulated owner-operators of the healthcare system but that have healthcare, cybersecurity and/or healthcare cybersecurity-specific expertise as consultants, law firms, security companies
- Advisor organization membership is capped at 15% of the Voting Membership
- Advisors are asked to join at least one task group and participate in at least 50% of the task group’s meetings
- Advisors are asked not to engage in any business development/sales activities while participating in HSCC business
- HSCC publications and communications cannot favor any vendor, technology or member relative to any other

Advisors neither vote nor hold CWG leadership positions, and join by invitation of leadership, subject to annual review.

Leadership

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, SVP Enterprise Technology Services & CISO, Novant Health

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, Chief of External Affairs, OCHIN, Inc.

MEDICAL TECHNOLOGY: Chris Reed, Sr. Director of Cybersecurity Policy, Global Regulatory Affairs, 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

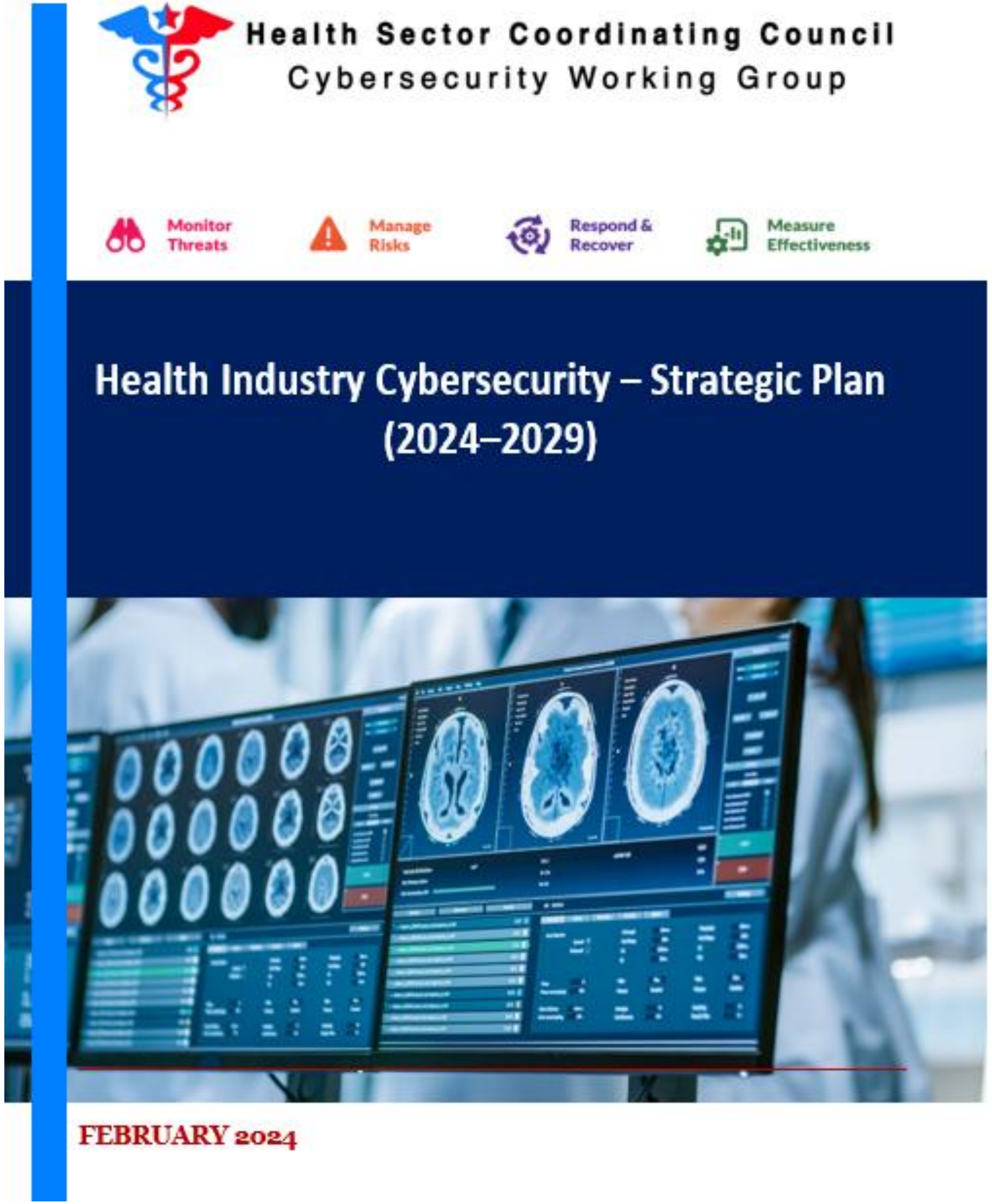
Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Sector Goals

2025 Priorities Under Consideration

- Organize and Implement Five-Year Cybersecurity Strategic Plan
- Complete Sector Mapping, Risk Assessment and Management Plan
- Recruit and Mobilize C-Suite leadership councils to accelerate sector-wide progress
- Continue development and promulgation of cybersecurity leading practices and policy recommendations

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



Health Sector Coordinating Council
Cybersecurity Working Group

Monitor Threats | Manage Risks | Respond & Recover | Measure Effectiveness

Health Industry Cybersecurity – Strategic Plan (2024–2029)

FEBRUARY 2024

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

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

Sector Mapping and Risk Assessment

Health Sector Coordinating Council
Cybersecurity Working Group

Cybersecurity Risk Assessment

Context

- **Technology systems are more complex and interconnected than ever before,** as a result of further integration and M&A activity across these systems
- **Cyberattacks on third party systems** introduce ever-expanding risk to the healthcare sector
- **This document reflects an assessment of systemic risks in healthcare services** brought on by cyber incidents to core technology systems

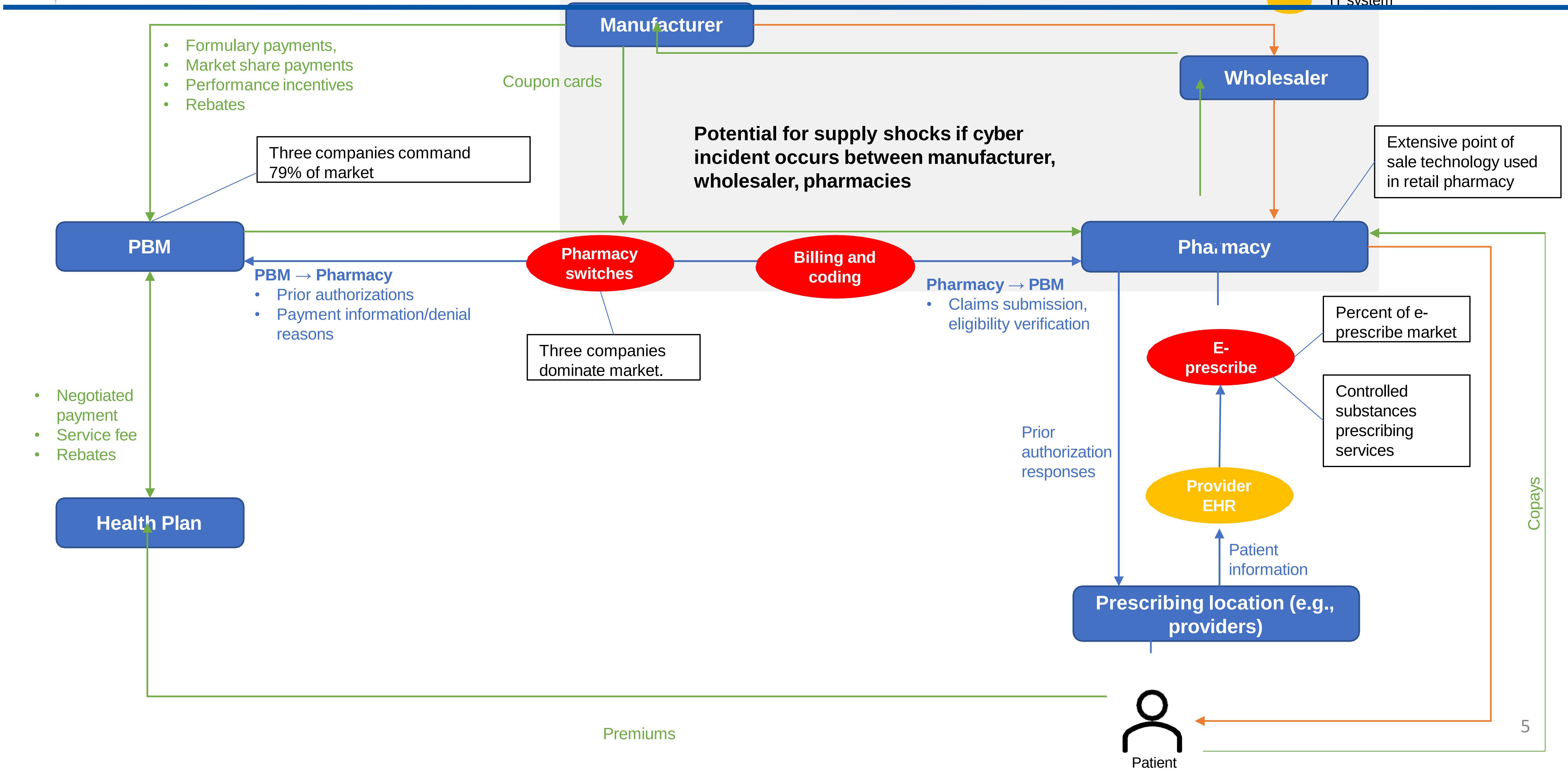
Objectives

- **Identify chokepoints in the healthcare system that could impact the flow of electronic health information, flow of payments, or the medical services** (e.g., medical care, pharmaceuticals, etc.)
- **Assess clinical, administrative, financial, and security impacts cybersecurity incidents** could have on healthcare system
- **Identify IT services and systems that service core functions for level and nature of impact, including:**
  - Retail pharmacy
  - Medical claims
  - Critical medical devices
  - Labs
  - Radiology
  - Dialysis
- **Assessment will be scoped to** systems, entities, and processes in the healthcare sector where prolonged outages from a cyber incident would result in significant sector-wide impacts

Example: Flow of Data and Payments in Retail Pharmacy

TLP RED

- 🟦 Entities
- 🔴 Third party service
- 🟡 IT system
- → Payments
- → EHI
- → Supply of drugs



Manufacturer

Wholesaler

PBM

Pharmacy

Health Plan

Prescribing location (e.g., providers)

Patient

Pharmacy switches

Billing and coding

E-prescribe

Provider EHR

- Formulary payments,
- Market share payments
- Performance incentives
- Rebates

Coupon cards

Potential for supply shocks if cyber incident occurs between manufacturer, wholesaler, pharmacies

Three companies command 79% of market

Extensive point of sale technology used in retail pharmacy

PBM → Pharmacy
- Prior authorizations
- Payment information/denial reasons

Three companies dominate market.

Pharmacy → PBM
- Claims submission, eligibility verification

Percent of e-prescribe market

Controlled substances prescribing services

- Negotiated payment
- Service fee
- Rebates

Prior authorization responses

Patient information

Copays

Premiums

How We Execute

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC Joint Cybersecurity Working Group
Task Groups Objectives And Leadership

TASK GROUP	OBJECTIVE	INDUSTRY LEADS	GOVT. LEAD
Artificial Intelligence Cybersecurity	Identify the emerging risks associated with the use of AI/ML based products and services in HPH and develop recommendations for their mitigations. Develop guidelines, standards, and best practices for AI safety and security.	**Rob Suarez** – *CareFirst* **Rohit Tandon –** *Essentia Health*	*HHS ASPR-* **Charlee Hess**
Health Industry Cybersecurity Landscape Analysis	Update 2023 Hospital Cybersecurity Landscape Analysis which identified the vulnerabilities and threats most frequently resulting in damaging attacks against hospitals and assesses the hospitals' known capabilities for preventing damaging cyber incidents. Version 2 of the L.A. will incorporate more data in the analysis and consider vulnerabilities and incidents faced by additional subsectors.	**Anahi Santiago** – *ChristianaCare* **James Case** – *Baptist Health NE Florida* **Ron Mehring –** *Texas Health Resources*	*HHS ASPR-* **Charlee Hess**
MedTech Cybersecurity Updating/Patching	Develop 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.	**Chris Gates -** *Velentium* **Phil Englert** – *Health ISAC*	*HHS FDA –* **Lisa Gilbert**
MedTech Manufacturing OT Cybersecurity	Developing leading practices for cybersecurity management of operational/manufacturing technology. Initially focused on medical technology and pharmaceutical subsectors.	**Edison Alvarez** - *Becton Dickinson* **Erin Gilliam** - *Merck*	*HHS FDA –* **Jessica Wilkerson**
MedTech Vulnerability Communications	Provide guidance to differing stakeholders (MDMs, HDO's, clinicians, patients) on 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.	**Kevin Tambascio** - *Cleveland Clinic* **Les Gray** - *Abbott* (Advisor) **Axel Wirth** - *Medcrypt*	*HHS FDA –* **Jessica Wilkerson**
Outreach and Awareness	Develop CWG brand and marketing strategy	**Kristi Warner** – *Abbott* **Ed Gaudet** – *Censinet* (Advisor)	*HHS HC3 –* **Troy Adams**

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC Joint Cybersecurity Working Group
Task Groups Objectives And Leadership

TASK GROUP	OBJECTIVE	INDUSTRY LEADS	GOVT. LEAD
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.	**Dr. Leanne Field** – *The UT Austin*	*HHS ASPR –* **Bob Bastani**
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	**Bryan Cline** – *HITRUST*	**TBD**
Sector Mapping and Risk Template	Develop methodology to identify chokepoints in the healthcare system that could impact the flow of electronic health information, payments, or medical services for core healthcare delivery and ancillary functions. Assess clinical, administrative, and financial impacts of cybersecurity incidents against and through third party entities. Integrate findings into third party and sector risk assessment and management plan	**Adrian Mayers –***Premera Blue Cross* **Samantha Jacques** – *McLaren Health*	*HHS ASPR -* **Charlee Hess**
Strategic Plan Implementation	Organized Health Industry Cybersecurity Strategic Plan into an implementation structure, process and timeline to achieve its 10 Goals and 12 Objectives by the target of 2029	**Chris Tyberg** – *Abbott* **Bobby Rao** – *Esper Group*	*FDA –* ***Linda Ricci***
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	**Jennifer Stoll** – *OCHIN, Inc.* **Jim Roeder** – *Lakewood Health System*	*DHS CISA NRMC* **Dr. Reuven Pasternak**

Health Sector Coordinating Council
Cybersecurity Working Group

JCWG Leading Practices
By the Sector for the Sector

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
- 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

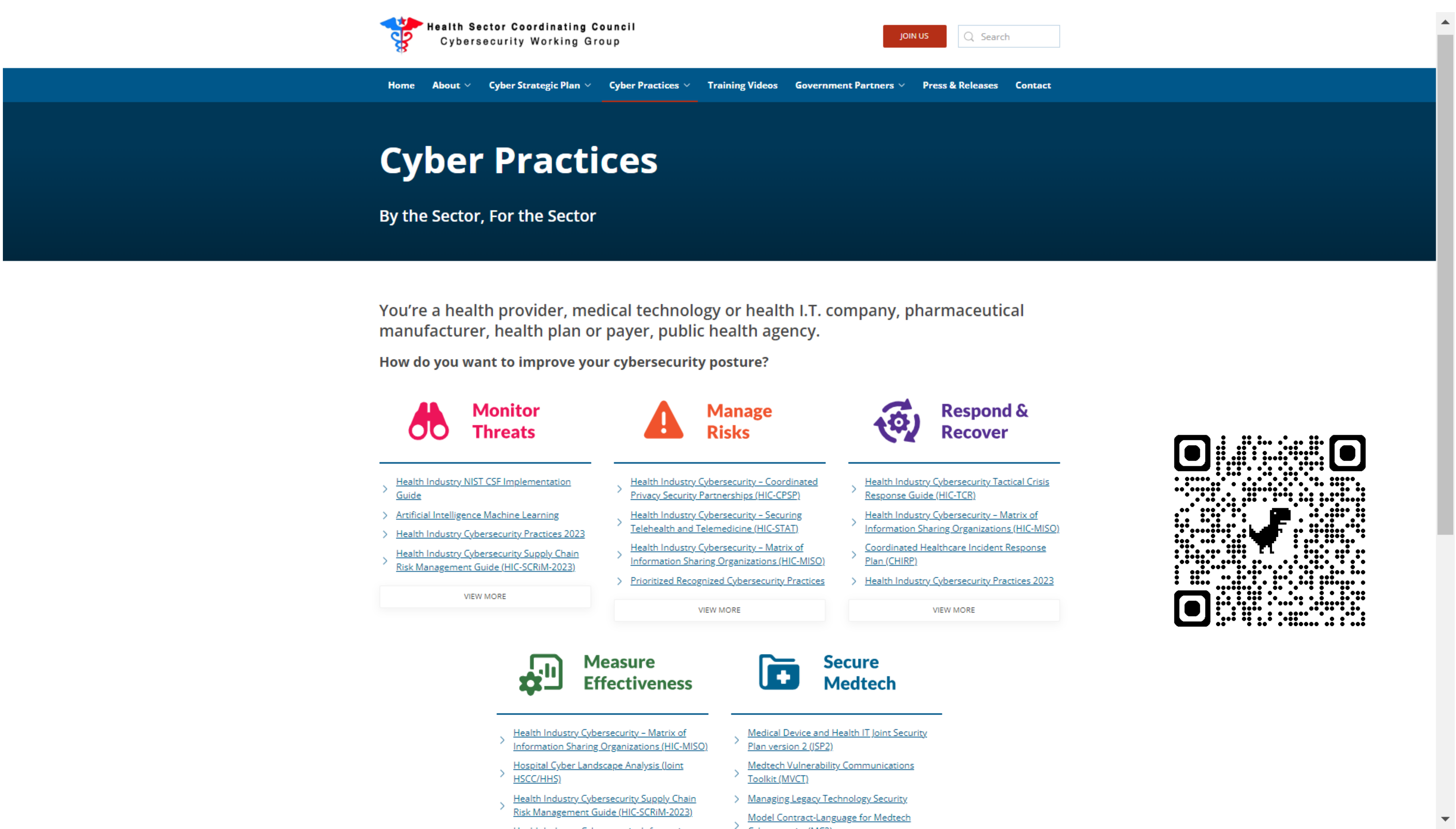
2020

- 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



Health Sector Coordinating Council
Cybersecurity Working Group

Cyber Practices

By the Sector, For the Sector

You're a health provider, medical technology or health I.T. company, pharmaceutical manufacturer, health plan or payer, public health agency.

How do you want to improve your cybersecurity posture?

Monitor Threats

- Health Industry NIST CSF Implementation Guide
- Artificial Intelligence Machine Learning
- Health Industry Cybersecurity Practices 2023
- Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM-2023)

VIEW MORE

Manage Risks

- Health Industry Cybersecurity – Coordinated Privacy Security Partnerships (HIC-CPSP)
- Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)
- Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO)
- Prioritized Recognized Cybersecurity Practices

VIEW MORE

Respond & Recover

- Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)
- Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO)
- Coordinated Healthcare Incident Response Plan (CHIRP)
- Health Industry Cybersecurity Practices 2023

VIEW MORE

Measure Effectiveness

- Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO)
- Hospital Cyber Landscape Analysis (Joint HSCC/HHS)
- Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM-2023)

Secure Medtech

- Medical Device and Health IT Joint Security Plan version 2 (JSP2)
- Medtech Vulnerability Communications Toolkit (MVCT)
- Managing Legacy Technology Security
- Model Contract-Language for Medtech

Next All-Hands Membership Meeting

November 19-21, 2024

Hosted at and Partnered with

University of California San Diego
Center for Healthcare Cybersecurity

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