Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks | Monitor Threats | Respond & Recover

Health Industry Cybersecurity -

Matrix of Information Sharing Organizations (HIC-MISO)

AUGUST 2023

Table of Contents

About the Health Sector Coordinating Council Cybersecurity Working Group

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is the largest HSCC working group of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely-available healthcare cybersecurity best practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

Purpose of the HIC-MISO

This guide identifies many of the information sharing organizations and their key services. Many health organizations are beginning to understand the importance of cybersecurity information sharing, but don't know where to start. Many cyber information sharing organizations exist and each plays a different or interdependent role. When a health organization is new to information sharing, it can be confusing to navigate these sharing organizations and their services, and how to engage with them in a way that reduces risk for the organization.

This resource does not necessarily represent an HSCC Joint Cybersecurity Working Group endorsement of the listed organizations, but a good faith effort to compile an inventory of established private sector and government organizations that publicly offer information sharing activities for the betterment of health industry cybersecurity awareness and resilience.

Building a Cybersecurity Sharing System into your Organization

Incorporation of information sharing into your organization's cybersecurity practices can be daunting, especially when you consider the number of potential sources you may have for information. If your organization does not have an information sharing plan in place, here is a short list of steps you can take to begin:

A follow-on project of the HSCC CWG will develop best practices for building an information sharing system into your organization's cyber risk management program. For the time being, the following is a short list of steps you can take to begin the process if your organization does not already have an enterprise information sharing program in place:

1. **Research available sources of information.** This guide is a great place to start. In addition, you should consider talking to the major vendors that you work with about how they supply information, and if they are members of a particular information sharing organization. There are also some services, free and paid, that may provide you with basic cybersecurity information as you develop your processes.
2. **Create an information flow chart.** A flow chart should, at minimum, show: who will receive shared cybersecurity information from your sources, how they will evaluate it, and the actions that should be taken as a result of evaluation. Don't be afraid to start simple! The process will mature as you perform it.

3. **Adjust your sources & process.** Cybersecurity is a journey, and information sharing is no different. It is easy to feel overwhelmed with options. Remember to start small, with what you consider to be the most important information, and then to expand as you gain confidence in the new system.

Download

Download a PDF version of the HIC-MISO here.

Guide to Information Cybersecurity Sharing Organizations for the Health Sector

Jump To

Health Sector Specific	Broad (Cross-Sector)
1. HHS ASPR	1. DHS NCCIC
2. HHS HC3	2. DHS C^3
3. HEALTH-ISAC	3. DHS US-CERT
4. HITRUST	4. DHS CISA
5. Med ISAO	5. DHS NICC
6. HPH-SCC	6. DHS NRMC
7. HPH Joint Cybersecurity Working Group	7. DHS HSIN
8. CHWG	8. DHS CISCP
9. AdvaMed MedTech ISAO	9. DHS AIS
10. PHEALTH-ISAC	10. DHS CSA
	11. FBI InfraGard
	12. CIS
	13. Sensato
	14. MITRE CWE
	15. MS-ISAC
	16. ISAO.org

Legend

F = Free

M = Included in Membership

A = A-La-Carte

R = Region Specific

Organization	HHS ASPR
Organization Type	Federal Government
Mission/Function	ASPR leads the Sector Specific Agency activities for Health & Human Services to protect the Healthcare and Public Health Sector from all hazards such as terrorism, infectious disease outbreaks, natural disasters and Cyber incidents. ASPR leads the nation's medical and public health preparedness for, response to, and recovery from disasters and public health emergencies. ASPR collaborates with hospitals, healthcare coalitions, biotech firms, community members, state, local, tribal, and territorial governments, and other partners across the country to improve readiness and response capabilities.
Notes	ASPR TRACIE Cybersecurity Collection – https://www.asprtracie.hhs.gov/technical-resources/86/cybersecurity/60 ASPR Critical infrastructure – https://www.phe.gov/Preparedness/planning/cip/Pages/default.aspx Free CIP Email Distribution (To include HC3 Briefings) – https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A

Broad Threat Intelligence Briefings	N/A	Health Sector-specific Threat Intelligence Briefings	F
*HPH-SCC Member	Yes		

Organization	HHS HCS
Organization Type	Federal Government
Mission/Function	The Health Sector Cybersecurity Coordination Center (HC3) is an operational cybersecurity center designed to support and improve the cyber defense of the healthcare and public health (HPH) sector. HC3, serves as HHS's nexus for cybersecurity collaboration with the HPH Sector, ensuring cybersecurity risks are actively identified and communicated out to sector partners.
Notes	Distribution through HEALTH-ISAC/CHWG/ASPR CIP

Broad Threat Intelligence Automated Feed	N/A	Health Sector-specific Threat Intelligence Automated Feed	F
Broad Threat Intelligence Email Distribution	N/A	Health Sector-specific Threat Intelligence Email Distribution	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing	F
Broad Threat Intelligence Live Analyst Chat	N/A	Health Sector-specific Threat Intelligence Live Analyst Chat	F

Broad Threat Intelligence Briefings	N/A	Health Sector-specific Threat Intelligence Briefings	F
*HPH-SCC Member	Yes		

Organization	HEALTH-ISAC
Organization Type	Private, Non profit.
Mission/Function	Offers healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other.
Notes	Items applicable to membership. TLP:GREEN distribution available to anyone within sector.

Broad Threat Intelligence Automated Feed	M	Health Sector-specific Threat Intelligence Automated Feed	M
Broad Threat Intelligence Email Distribution	F	Health Sector-specific Threat Intelligence Email Distribution	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	M	Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing	M
Broad Threat Intelligence Live Analyst Chat	M	Health Sector-specific Threat Intelligence Live Analyst Chat	M

Broad Threat Intelligence Briefings	M	Health Sector-specific Threat Intelligence Briefings	M
*HPH-SCC Member	Yes		

Organization	HITRUST (in partnership with Cysiv)
Organization Type	Private, Non profit.
Mission/Function	Not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain.
Notes	

Broad Threat Intelligence Automated Feed	M	Health Sector-specific Threat Intelligence Automated Feed	M
Broad Threat Intelligence Email Distribution	M	Health Sector-specific Threat Intelligence Email Distribution	M
Broad Threat Intelligence Analyst to Analyst Email Sharing	M	Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing	M
Broad Threat Intelligence Live Analyst Chat	M	Health Sector-specific Threat Intelligence Live Analyst Chat	M

Broad Threat Intelligence Briefings	M	Health Sector-specific Threat Intelligence Briefings	M
*HPH-SCC Member	Yes		

Organization	Med ISAO
Organization Type	Private, Non profit.
Mission/Function	Med ISAO provides cybersecurity information, education and tools tailor-made for the medical device industry. Med ISAO runs a coordinated vulnerability disclosure program.
Notes	In addition to health sector based feeds, Med ISAO also offer customizable feeds that can be tailored to specific medical devices technologies.

Broad Threat Intelligence Automated Feed	N/A	Health Sector-specific Threat Intelligence Automated Feed	M
Broad Threat Intelligence Email Distribution	N/A	Health Sector-specific Threat Intelligence Email Distribution	M
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing	M
Broad Threat Intelligence Live Analyst Chat	N/A	Health Sector-specific Threat Intelligence Live Analyst Chat	N/A

Broad Threat Intelligence Briefings	N/A	**Health Sector-specific Threat Intelligence Briefings**	M
***HPH-SCC Member**	No		

Organization	Center for Internet Security (CIS)
Organization Type	Private, Non profit.
Mission/Function	Non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. The go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities. CIS also operates MS-ISAC.
Notes	Requires membership for many services but CIS Benchmarks are available for free.

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	M	**Health Sector-specific Threat Intelligence Email Distribution**	N/A
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A

Broad Threat Intelligence Briefings	M	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	No		

Organization	Sensato
Organization Type	Private
Mission/Function	Sensato's Information Sharing & Analysis Organization (ISAO) deploys sensors on client networks, monitoring the traffic coming across the wire so that we can quickly detect suspicious behavior. Sensato is an active part of a wider intelligence community to keep ourselves and our client members up-to-date on and protected from the most recent cybersecurity threats. We are a member of the Department of Homeland Security Cybersecurity Initiative, have signed an MOU with the Food and Drug Administration (FDA), and receive intelligence from the Federal Bureau of Investigations (FBI).
Notes	We also provide healthcare specific incident response support using a "ability to pay" model.

Broad Threat Intelligence Automated Feed	M	**Health Sector-specific Threat Intelligence Automated Feed**	M
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F

Broad Threat Intelligence Live Analyst Chat	F	Health Sector-specific Threat Intelligence Live Analyst Chat	F
Broad Threat Intelligence Briefings	F	Health Sector-specific Threat Intelligence Briefings	F
*HPH-SCC Member	Yes		

Organization	DHS National Cybersecurity and Communications Center (NCCIC)
Organization Type	Federal Government
Mission/Function	NCCIC is a hub for information and expertise. We are a global exchange for cyber and communications information, sharing what we receive back to the cyber security community.
Notes	Many of these categories are available pending organizations partner level and participation, CISCP, ICWG, ATTE, HSIN access, AIS etc.

Broad Threat Intelligence Automated Feed	F	Health Sector-specific Threat Intelligence Automated Feed	F
Broad Threat Intelligence Email Distribution	F	Health Sector-specific Threat Intelligence Email Distribution	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing	F

Broad Threat Intelligence Live Analyst Chat	F	**Health Sector-specific Threat Intelligence Live Analyst Chat**	F
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	F
***HPH-SCC Member**	DHS is a member		

Organization	DHS Critical Infrastructure Cyber Community C^3 Voluntary Program
Organization Type	Federal Government
Mission/Function	Supports owners and operators of critical infrastructure, academia, Federal government, State, Local, Tribal, and Territorial (SLTT) governments, and business in their use of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework), an industry-developed voluntary framework to help organizations address and improve their cybersecurity risk management.
Notes	To receive email updates from the DHS C3 – https://www.us-cert.gov/mailing-lists-and-feeds.

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	F
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F

Broad Threat Intelligence Live Analyst Chat	F (HSIN)	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	No
***HPH-SCC Member**	DHS is a member		

Organization	DHS US-CERT (HIRT & NCCIC)
Organization Type	Federal Government
Mission/Function	Reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.
Notes	

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F

Broad Threat Intelligence Live Analyst Chat	F	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	DHS is a member		

Organization	DHS CISA
Organization Type	Federal Government
Mission/Function	CISA's Cybersecurity Division leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector – the ".com" domain – to increase the security of critical networks.
Notes	AIS/ECS

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	F
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F

Broad Threat Intelligence Live Analyst Chat	F	Health Sector-specific Threat Intelligence Live Analyst Chat	F
Broad Threat Intelligence Briefings	F	Health Sector-specific Threat Intelligence Briefings	F
*HPH-SCC Member	DHS is a member		

Organization	DHS CISA NICC
Organization Type	Federal Government
Mission/Function	The dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets.
Notes	

Broad Threat Intelligence Automated Feed	F	Health Sector-specific Threat Intelligence Automated Feed	F
Broad Threat Intelligence Email Distribution	F	Health Sector-specific Threat Intelligence Email Distribution	F

Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	DHS is a member		

Organization	DHS CISA National Risk Management Center (NRMC)
Organization Type	Federal Government
Mission/Function	The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions.
Notes	

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	N/A	**Health Sector-specific Threat Intelligence Email Distribution**	N/A

Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	DHS is a member		

Organization	DHS HSIN COI's
Organization Type	Federal Government
Mission/Function	The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, State, Local, Territorial, Tribal, International and Private Sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.
Notes	Additional information on HSIN can be found here: https://www.dhs.gov/homeland-security-information-network-hsin.

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	F
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F

Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F
Broad Threat Intelligence Live Analyst Chat	F	**Health Sector-specific Threat Intelligence Live Analyst Chat**	F
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	F
***HPH-SCC Member**	DHS is a member		

Organization	DHS CISA Cyber Information Sharing and Collaboration Program (CISCP)
Organization Type	Federal Government
Mission/Function	CISCP enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners.
Notes	Additional information on CISCP can be found here: https://www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp.

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	F

Broad Threat Intelligence Email Distribution	F	Health Sector-specific Threat Intelligence Email Distribution	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing	F
Broad Threat Intelligence Live Analyst Chat	F	Health Sector-specific Threat Intelligence Live Analyst Chat	F
Broad Threat Intelligence Briefings	F	Health Sector-specific Threat Intelligence Briefings	F
*HPH-SCC Member	DHS is a member		

Organization	DHS Automated Indicator Sharing (AIS) Program
Organization Type	Federal Government
Mission/Function	AIS is a capability CISA has developed to enable the exchange of cyber threat indicators between private sector entities and government departments and agencies at machine speed, which will allow participants to mitigate cyber threats in near-real-time.
Notes	

Broad Threat Intelligence Automated Feed	F	Health Sector-specific Threat Intelligence Automated Feed	F

Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F
Broad Threat Intelligence Live Analyst Chat	F	**Health Sector-specific Threat Intelligence Live Analyst Chat**	F
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	F
***HPH-SCC Member**	DHS is a member		

Organization	DHS Cybersecurity Advisory (CSA) Program
Organization Type	Federal Government
Mission/Function	The Department of Homeland Security's (DHS) Cybersecurity Advisors (CSAs) offer assistance to help prepare and protect private sector entities and SLTT governments from cybersecurity threats. CSAs promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities.
Notes	For more information about the CSA Program or to inquire about your region's CSA, please email cyberadvisor@hq.dhs.gov.

Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	F

Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F
Broad Threat Intelligence Live Analyst Chat	F	**Health Sector-specific Threat Intelligence Live Analyst Chat**	F
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	F
***HPH-SCC Member**	DHS is a member		

Organization	FBI InfraGard
Organization Type	Private–FBI (DOJ) and private partnership
Mission/Function	The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure.
Notes	To become a member you must apply through your local chapter.

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A

Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	N/A
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	F	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	N/A	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	Yes		

Organization	Healthcare and Public Health Sector Coordinating Council (HPH-SCC)
Organization Type	Private, Non profit.
Mission/Function	Coordinates deliberations between healthcare owners and operators and government leaders toward policy and systemic improvements to the security and resilience of critical healthcare infrastructure.
Notes	

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A

Broad Threat Intelligence Email Distribution	N/A	**Health Sector-specific Threat Intelligence Email Distribution**	M
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	M	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	Yes		

Organization	HPH Joint Cybersecurity Working Group
Organization Type	Private, Non profit.
Mission/Function	The largest standing working group of the HPH SCC, the JCWG coordinates deliberations between healthcare owners and operators and government leaders toward cybersecurity policy and systemic improvements to the security and resilience of critical healthcare infrastructure.
Notes	

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A

Broad Threat Intelligence Email Distribution	N/A	**Health Sector-specific Threat Intelligence Email Distribution**	N/A
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	F	**Health Sector-specific Threat Intelligence Briefings**	F
***HPH-SCC Member**	Yes		

Organization	MITRE Common Weaknesses and Enumerations DB (MITRE CWE)
Organization Type	Private, Non-profit
Mission/Function	CWE is a community-developed formal list of common software weaknesses. It serves as a common language for describing software security weaknesses, a standard measuring stick for software security tools targeting these vulnerabilities, and as a baseline standard for weakness identification, mitigation, and prevention efforts. Leveraging the diverse thinking on this topic form academia, the commercial sector, and government, CWE unites the most valuable breadth and depth of content and structure to serve as a unified standard. Our objective is to help shape and mature the code security assessment industry and also dramatically accelerate the use and utility of software assurance capabilities for organizations in reviewing the software systems they acquire or develop.
Notes	CWE is often included in other threat intelligence products, so even though the CWE list doesn't provide a broad range of services it may be included in some of the threat intelligence services provided by other organizations in this matrix.

	For more information: https://cwe.mitre.org/about/		
Broad Threat Intelligence Automated Feed	F	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	N/A	**Health Sector-specific Threat Intelligence Email Distribution**	N/A
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	N/A
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	N/A	**Health Sector-specific Threat Intelligence Briefings**	N/A
***HPH-SCC Member**	Yes		

Organization	Cyber Health Working Group
Organization Type	Private, Non-profit
Mission/Function	The Cyber Health Working Group maintains a web-based platform which provides tools for its members to share cyber threat information and resources. It also hosts a monthly webinar focused on a specific cyber threat, training topic, best practice, or threat mitigation solution in the health sector

Notes	The CHWG was originally created by the National Capital Region chapter of InfraGard (InfraGard NCR) and the Cyber Task Force (CTF) at the FBI's Washington Field Office but is now part of the Cyber Forensic Training Alliance.

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	F	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	F
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	N/A
Broad Threat Intelligence Briefings	N/A	**Health Sector-specific Threat Intelligence Briefings**	F
***HPH-SCC Member**	No		

Organization	Multi-State Information Sharing & Analysis Center MS-ISAC (Center for Internet Security)
Organization Type	Private, Non-profit
Mission/Function	Improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Notes	Only applicable to public health entities for membership. TLP:WHITE distribution available to anyone.

Broad Threat Intelligence Automated Feed	M	**Health Sector-specific Threat Intelligence Automated Feed**	M
Broad Threat Intelligence Email Distribution	M	**Health Sector-specific Threat Intelligence Email Distribution**	M
Broad Threat Intelligence Analyst to Analyst Email Sharing	M	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	M
Broad Threat Intelligence Live Analyst Chat	M	**Health Sector-specific Threat Intelligence Live Analyst Chat**	M
Broad Threat Intelligence Briefings	M	**Health Sector-specific Threat Intelligence Briefings**	M
***HPH-SCC Member**	No		

Organization	AdvaMed MedTech ISAO
Organization Type	Private, Non-profit
Mission/Function	To enhance information sharing among medical device manufacturers and implement one of its foundational cybersecurity principles, the Advanced Medical Technology Association (AdvaMed) hosts the medical technology information sharing and analysis organization (MedTech ISAO). The MedTech ISAO enables AdvaMed members to voluntarily share

	information relating to cybersecurity threats, vulnerabilities, incidents and mitigations in a safe and secure environment.
Notes	The MedTech ISAO provides an online forum for medical technology organizations to collaborate and exchange cybersecurity-related information, develop and share industry best practices, and discuss and evaluate key components of an effective cybersecurity plan.

Broad Threat Intelligence Automated Feed	N/A	**Health Sector-specific Threat Intelligence Automated Feed**	N/A
Broad Threat Intelligence Email Distribution	N/A	**Health Sector-specific Threat Intelligence Email Distribution**	M
Broad Threat Intelligence Analyst to Analyst Email Sharing	N/A	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	M
Broad Threat Intelligence Live Analyst Chat	N/A	**Health Sector-specific Threat Intelligence Live Analyst Chat**	M
Broad Threat Intelligence Briefings	N/A	**Health Sector-specific Threat Intelligence Briefings**	M
***HPH-SCC Member**	Yes		

Organization	ISAO.org
Notes	For a complete listing of healthcare ISAOs, ISAO.org offers a directory of all ISAOs, some of which are in the healthcare sector.

Organization	PHEALTH-ISAC at CommHIT
Organization Type	Private, Non-profit
Mission/Function	CommHIT's Population Health Information Sharing and Analysis Center (PHEALTH-ISAC) and Community & Transportation ISAC (C&T-ISAC) work for businesses and organizations that serve the healthcare and social service needs of underserved populations. PHEALTH-ISAC and C&T-ISAC help members meet regulatory requirements, reduce cyber risk, and identify cyber threats.
Notes	To join, write CommHIT at info@communityhealthit.org

Broad Threat Intelligence Automated Feed	M	**Health Sector-specific Threat Intelligence Automated Feed**	M
Broad Threat Intelligence Email Distribution	F	**Health Sector-specific Threat Intelligence Email Distribution**	F
Broad Threat Intelligence Analyst to Analyst Email Sharing	M	**Health Sector-specific Threat Intelligence Analyst to Analyst Email Sharing**	M
Broad Threat Intelligence Live Analyst Chat	M	**Health Sector-specific Threat Intelligence Live Analyst Chat**	M
Broad Threat Intelligence Briefings	M	**Health Sector-specific Threat Intelligence Briefings**	M
***HPH-SCC Member**	Yes		

Footnotes

The HPH-SCC is recognized by the Secretary of Health and Human Services as the critical infrastructure industry partner with the government under Presidential Policy Directive 21 for coordinating strategic and policy approaches to preparing for, responding to, and recovering from significant cyber and physical threats to the sector. These include natural, technological and manmade disasters, and national or regional health crises. Its mission is to collaborate with the Department of Health and Human Services and other federal agencies to develop and encourage adoption of recommendations and guidance for policy, regulatory and market-driven strategies to facilitate collective mitigation of cybersecurity threats to the sector that affect patient safety, security, and privacy, and consequently, national confidence in the healthcare system.