



Health Sector Coordinating Council Cybersecurity Working Group

Health Sector Publishes Framework A.I. Cybersecurity Governance

New resource by the sector's primary critical infrastructure advisory council helps healthcare organizations create and manage enterprise cybersecurity governance for AI

Washington, DC – June 1, 2026

Today the Cybersecurity Working Group (CWG) of the Health Sector Coordinating Council (HSCC) published a guide to help healthcare organizations (HCOs) establish cyber governance frameworks for secure AI implementation. The "[Health Industry AI Cyber Governance Framework Implementation Guide](#)" addresses unique cybersecurity and privacy challenges as the sector adopts artificial intelligence across clinical and operational use cases, targeting the identification and mitigation of AI-specific cyber risks, including data poisoning, model drift, and adversarial attacks, while ensuring compliance with the healthcare sector's complex regulatory environment. It addresses the full spectrum of AI technologies deployed in healthcare, from traditional machine learning/reactive/non-agentic models to generative AI, and agentic AI systems capable of autonomous action.

The Guide focuses on the cybersecurity dimensions of AI governance: protecting AI systems from adversarial threats, ensuring data integrity and privacy, securing the AI supply chain, and maintaining operational resilience. Topics such as clinical safety, ethics, and patient engagement are addressed to the extent that they intersect with cybersecurity risk. Organizations should maintain a broader AI governance program that addresses the full spectrum of AI risks beyond cybersecurity in the ever-changing ecosystem.

It also complements other HSCC AI-specific publications and should be considered as part of a larger volume of work developed to guide the health industry in its safe and secure adoption of AI. Specifically, this document will significantly reference the [Health Industry Third-Party AI Risk and Supply Chain Transparency Guide](#) published April 15 2026 and should be used in conjunction with this publication.

Standardizing Terminology

Alongside today's release of the Guide, the HSCC Cybersecurity Working Group's AI Task Group references its [AI Cyber Glossary](#) - a living reference document establishing consistent, governance-ready definitions for artificial intelligence terminology across the health sector.

The glossary was developed in direct response to a critical gap in managing healthcare AI and AI cybersecurity: the absence of shared, sector-specific language that clinical, operational, compliance, and technical stakeholders can use with confidence. As AI adoption accelerates across healthcare organizations of every size, inconsistent terminology creates real risk - in procurement decisions, vendor contracts, regulatory submissions, policy development, and patient safety oversight. As a living document the Glossary is designed to serve as the terminological foundation for all current and future HSCC AI Task Group guidance materials.

About the HSCC CWG

The [Health Sector Coordinating Council \(HSCC\) Cybersecurity Working Group \(CWG\)](#) is a government-recognized critical-infrastructure industry advisory council of almost 500 healthcare organizations in health delivery; life sciences, lab and medical technology; health insurance and plans; health I.T. and information exchange; public health and government agencies partnering to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership develops and publishes free healthcare [cybersecurity leading practices](#) and policy recommendations, and promotes the imperative that **cyber safety is patient safety**.

More information: <https://HealthSectorCouncil.org/Contact>