



Health Sector Coordinating Council Cybersecurity Working Group

Health Sector Publishes Guide for Third-Party A.I. Cybersecurity

New resource by the sector for the sector helps healthcare organizations manage AI-enabled third-party technology and services that need cybersecurity oversight

Washington, DC – April 15, 2026

Today the Cybersecurity Working Group (CWG) of the Health Sector Coordinating Council (HSCC) is providing healthcare organizations with best practices to address the realities of AI-driven supply chains in healthcare.

The healthcare sector's accelerating adoption of artificial intelligence has expanded its dependence on third-party tools and services, introducing complex cybersecurity challenges that traditional risk management tools and models struggle to address. From natural language processing engines embedded in electronic health records (EHRs) to AI-driven remote monitoring devices, many critical functions rely on external vendors whose security postures, data governance practices, and model integrity are difficult to verify. Compounding the risk, healthcare organizations (HCOs) often lack visibility into the full scope of AI components sourced through layered supply chains, including subcontractors, offshore development, and open-source AI assets. This opacity elevates systemic exposure and risk, further complicating response coordination in the event of a breach or model failure.

Crucially, this new publication - the "*Health Industry Third-Party AI Risk and Supply Chain Transparency Guide*" - addresses the growing gaps in discovery and disclosure processes that make AI supply chain risk so difficult to manage. Many HCOs operate with incomplete or outdated vendor inventories, while AI-specific cybersecurity risks - such as synthetic data misuse, training data leakage, and adversarial inference - go unreported by vendors. To counter this, the Guide promotes proactive due diligence, dynamic risk profiling, and contractual transparency. It equips risk managers, compliance teams, and procurement officers with scalable tools to surface hidden dependencies, identify cascading failure points, and align third-party AI vendors and products with mission-critical safety, privacy, and resilience goals.

Standardizing Terminology

Alongside today's release of the Guide, the HSCC Cybersecurity Working Group's AI Task Group is publishing 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 more than 480 healthcare organizations in health delivery; life sciences, lab and medical technology; health insurance and plans; health I.T. and information exchange; and 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>

##