Health Sector Coordinating Council
Cybersecurity Working Group

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

Health Industry Cybersecurity

Artificial Intelligence
2026 Guidance Previews

November 2025

Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Publishes Previews for A.I. Cybersecurity Guidance

Complexity of AI Cybersecurity Opportunities and Challenges Requires Phased Rollout of Resources Focusing on Components of Good AI Cybersecurity Policy and Practices

Washington, DC – November 11, 2025

Today the Cybersecurity Working Group (CWG) of the Health Sector Coordinating Council (HSCC) is providing the healthcare sector a preview of soon-to-be published resources focusing on discrete but interrelated functional imperatives for managing A.I. cybersecurity challenges and opportunities in the healthcare system. The introductory compilation of A.I. one-page summaries can be found on the HSCC Cybersecurity website at *https://healthsectorcouncil.org/ai-cybersecurity-onepagers/*.

Given the cybersecurity challenges and opportunities presented by artificial intelligence The HSCC CWG formed an AI Cybersecurity Task Group in October 2024 composed of 115 healthcare organizations across the spectrum to consider how to prepare the sector with operational and organizational guidance. The AI Task Group recognized the complexity and associated risk of A.I. technology used in clinical, administrative and financial health sector applications, and accordingly divided the mix of AI issues into manageable work streams of discrete functional areas of concentration while staying mindful of the interrelationships and interdependencies among those functions. The effort is separated into five subgroups:

Education and Enablement
Common nomenclature for our AI cybersecurity guidance, and education and training programs to familiarize diverse healthcare user communities with the appropriate awareness and use of AI in their functional environments.

Cyber Operations & Defense
Practical playbooks to help healthcare organizations to prepare for, detect, respond to, and recover from AI-related cyber incidents.

Governance
A comprehensive framework for managing AI cybersecurity risks in the health sector enterprise, including: governance processes for the AI lifecycle; regulatory alignment; and AI-specific security and data.

Secure by Design
Embedding cybersecurity secure-by-design principles into the DNA of AI-enabled medical devices, while fostering collaboration across engineering, cybersecurity, regulatory and clinical teams.

Third-Party AI Risk & Supply Chain Transparency
Strengthen security, trust and resilience in supply chains by enhancing visibility and transparency of third-party AI tools, establishing governance and oversight policies, and standardizing procurement, vendor vetting, and lifecycle management, among other deliverables.

Looking Ahead

These workstreams have made substantial progress over the past several months and beginning in January will separately publish their guidance documents in succession through Q1 2026. Today's announcement attaches to this release the line-up of one-page summaries of the objectives and deliverables of those subgroups as an advance overview of the suite of issues covered in this initiative. In addition, we offer as a bonus the first of our foundational publications developed by the Education and Enablement Subgroup – "A.I. in Healthcare: 10 Terms You Need to Know."

Call to Action

The HSCC CWG invites all healthcare organizations to adopt these best practices, share guidance across teams, and engage with the council to shape the future of sector-wide AI governance and cybersecurity. Together, we can ensure that innovation in healthcare is matched by a steadfast commitment to patient safety, data privacy and operational resilience.

About the HSCC Cybersecurity Working Group

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

##

Education and Enablement

Objective

Improve education and awareness of AI/ML technology to better understand risk and apply control activities

Key Focus Areas

- Definitions
- Terminology
- AI/Machine Language fundamentals
- Specific AI risks and mitigation.

Intended Deliverables and Outcomes

Deliverables include:

- Top 10 AI definitions
- AI assisted learning aides (videos, infographics, etc)
- Recommended education and courses

Outcomes include:

- Education and awareness for AI/ML terminology
- Understanding of the use of AI in healthcare
- Understanding risks of AI deployment and operations
- Broad application of appropriate controls

##

Cyber Operations and Defense

Objective

- Identify necessary requirements to effectively conduct optimized AI-specific cybersecurity operations to address issues in healthcare environments, including incident response and recovery.
- Define AI-driven threat intelligence processes with safeguards that support clinical workflows and broader health operations.
- Establish risk factors and operational guardrails for AI technologies beyond LLMs, such as predictive ML systems and embedded device AI.
- Develop a draft Playbook(s) structure and populate initial sections with discussion-driven content.
- Create recommendations for stakeholder roles and processes to iterate and mature the Playbook(s) over time.

Key Focus Areas

- Provide a structured framework for preparing, detecting, responding to, and recovering from AI-related cyber incidents while providing a best-practices approach to business continuity and regulatory compliance.
- Establish clear governance and accountability, integrating AI-specific risk assessments into existing cybersecurity frameworks, and defining tailored response procedures for threats such as model poisoning, data corruption, and adversarial attacks.
- Enable continuous monitoring of AI systems, ensure rapid containment and recovery of compromised models, and maintain secure, verifiable model backups.
- Emphasize the importance of resilience testing, cross-functional coordination between cybersecurity and data science teams, and continuous learning from incidents to strengthen future preparedness.

Intended Deliverables and Outcomes

- AI Cyber Resilience and Incident Recovery Playbook
- AI Driven Clinical Workflow Threat Intelligence Playbook
- Cybersecurity Operations for AI Systems Playbook

##

Governance Framework Implementation

Objective

Provide a comprehensive framework for healthcare organizations of all sizes to manage the unique cybersecurity risks of AI in a clinical environment. The goal is to govern the use of AI securely and responsibly.

Key Focus Areas

- **Establish a Governance Framework:** Create formal processes that define roles, responsibilities, and clinical oversight for the AI lifecycle.
- **Align with Regulations:** Map AI governance controls to legal and regulatory requirements like HIPAA and FDA rules.
- **Identify Standards and Controls:** Implement AI-specific security and data controls, referencing frameworks like the NIST AI Risk Management Framework.
- **Inventory AI Systems:** Develop a complete inventory of all AI systems to understand their function and data dependencies.
- **Apply Autonomy Levels:** Classify AI tools on a 5-level autonomy scale to match human oversight with system risk.

Intended Deliverable and Outcome

A guide that features an *AI Governance Maturity Model*. This model allows organizations to assess their capabilities, identify gaps, and prioritize improvements. The intended outcome is to ensure that AI is deployed *safely, ethically, and effectively* in healthcare.

##

Secure by Design Medical Devices

Objective

Define and develop Secure-by-Design principles *specifically tailored for AI-enabled medical devices*. This includes delivering practical guidance and tools that empower medical device manufacturers and stakeholders to embed cybersecurity throughout the entire product lifecycle.

Key Focus Areas

- **Address Unique AI Security Risks:** Highlight emerging threats such as data poisoning, model manipulation, and drift exploitation. Align mitigation strategies with leading regulatory frameworks, including U.S. FDA guidance, NIST AI Risk Management Framework (RMF), and CISA recommendations.
- **Enable Cross-Functional Collaboration:** Foster coordination across engineering, cybersecurity, regulatory affairs, quality assurance, and clinical teams to ensure AI specifics risks and activities are integrated throughout the medical device risk management process and development area.
- **Advance Transparency and Supply Chain Security:** Support the integration of AI Bill of Materials (AIBOM) and Trusted AI BOM (TAIBOM) to enhance visibility, traceability, scalability and trust across the AI supply chain.

Intended Deliverables and Outcomes

Establish a set of AI-specific security practices that span the entire AI lifecycle. These practices will be designed to support organizations of all sizes in securely integrating AI into medical device design. The key deliverables include:

- AI Secure by Design Guidance – actionable recommendations for embedding security into AI-enabled medical devices from the outset.
- AI Security Risk Taxonomy – a structured framework to identify, categorize, and assess AI-related security risks.
- Functional Role Implementation Briefs – tailored guidance for key stakeholders (e.g., developers, product managers, security teams) to operationalize AI security practices.
- Educational and Awareness Materials – resources to build organizational understanding and promote a security-first mindset in AI development.

##

Third Party Risk and Supply Chain Management

Objective

- Enhance Visibility & Transparency
- Establish Governance & Oversight
- Manage Cyber & Data Risks
- Contractual & Legal Safeguards
- Lifecycle Risk Management
- Promote Shared Responsibility
- Ethical & Responsible AI Use

Key Focus Areas

- Identify, track, and monitor third-party AI tools and supply chains.
- Define accountable policies, governance boards, and approval pathways.
- Evaluate third-party AI for security, privacy, and bias risks (NIST AI RMF, HICP, HIPAA).
- Standardize procurement, vendor vetting, monitoring, and end-of-life planning.
- Provide model contract/BAA clauses for data use, PHI handling, and breach reporting.
- Foster collaboration between healthcare organizations and AI vendors.
- Encourage bias testing, fairness, and human oversight in AI adoption.

Intended Deliverables and Outcomes

Implemented Guidance that:

- Reduces systemic exposure to hidden AI risks across layered vendor supply chains.
- Provides scalable tools and best practices for GRC, procurement, and compliance teams.
- Elevates patient safety, data privacy, and trust by embedding accountability and transparency.
- Ensures alignment with evolving regulatory requirements and global AI standards (NIST, FDA, ISO, IMDRF).

##

A.I. in Healthcare: 10 Terms You Need to Know

AI is everywhere in healthcare - from scheduling to diagnosing. It can save time and improve care, but it can also create new risks.

Here are the buzzwords you'll hear and what they mean…

AI Agents: AI that makes decisions or performs tasks without needing human input, for example Agentic AI.

Algorithm: Step-by-step instructions a computer follows to solve problems. Often used to refer to the mechanism by which an AI performs a task.

Artificial Intelligence (AI): Systems that mimic human intelligence to perform tasks.

Bias: When AI results are unfair due to errors in data or design.

Data Privacy: Protecting sensitive information, particularly patient information, used in AI systems.

Explainability: Being able to understand and explain how an AI system makes its decisions in a way that humans can follow.

Generative AI: AI that creates new content such as text, images, and video based on input and learned patterns.

Hallucination: When AI generates false or misleading information.

Large Language Model (LLM): AI trained on vast amounts of text to understand and generate language.

Machine Learning (ML): AI that learns patterns from data instead of being directly programme.

A.I. is a powerful tool in healthcare - but only if we use it wisely. Learn the basics, ask questions, and stay alert to both the value and the risks.

Cyber Safety is Patient Safety
https://HealthSectorCouncil.org