



Health Sector Publishes Updated Cybersecurity Model Contract

New model contract by the Cybersecurity Working Group builds on the 2022 version to align medical device manufacturers and health delivery organizations in cybersecurity contract negotiations

St. Louis, MO – November 18, 2025

Today during its semi-annual All-Hands Membership meeting hosted by University of Health Sciences and Pharmacy in St. Louis, the Cybersecurity Working Group (CWG) of the Healthcare and Public Health Sector Coordinating Council (HSCC) published an updated reference for shared cooperation and coordination between Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) regarding the security, compliance, management, operation, and services of medical technology in the clinical environment.

The Model Contract for Medtech Cybersecurity version 2 (MC²v.2) is intended to minimize security risks and ensure the confidentiality, integrity, and availability of HDO healthcare technologies, infrastructures, and information. MC²v.2 articulates security terms and conditions for HDO information being stored, transferred, or accessed and provides that all network access, medical products, services, and solutions satisfy the mission, security, safety, and compliance requirements of the HDO. This version 2 integrates feedback about the experience of healthcare stakeholders in implementing the original March 2022 version and adds new contract clauses to address gaps in the first contract.

Why a Model Contract?

Understanding and management of medical product cybersecurity responsibility and accountability between MDMs and HDOs is complicated by many conflicting factors, including uneven MDM capabilities and investment in cybersecurity controls built into product design and production; varying expectations for cybersecurity among HDOs; and high cybersecurity management costs in the HDO operational environment throughout the product lifecycle. These factors have introduced and sustained ambiguities in cybersecurity accountability between MDM's and HDO's that historically have been inconsistently reconciled in the purchase contract negotiation process, leading to downstream disputes, insufficient security and, potentially, patient safety concerns.

To strengthen clarity of mutual obligations between parties to a contract, the parties first need clear alignment to existing standards, simplification of cybersecurity requirements, and scalable cybersecurity best practices for easy access and adoption. These best practices are finding their way into the healthcare industry, through recent HSCC Cybersecurity Working Group CWG publications such as the [Health Industry Cybersecurity Practices \(HICP\)](#) for healthcare providers and the [Medical Device and Health IT Joint Security Plan v2 \(JSP2\)](#) as a guide for MDM cybersecurity design and production. With these practices and others as foundations for mature cybersecurity risk management, purchase contract negotiations will have clearer references for obligations, accountability and liability. It is in this context that this HSCC CWG Model Contract-language for Medtech Cybersecurity Version 2 (MC²v.2 or "MC Squared") resource is offered as an update to the original MC² published in March 2022.

Refinements in MC2 v.2

MC²v2 makes improvements to the original MC²v1 by:

- Incorporating feedback received for MC2 v.1;
- Revising and expanding content to align with changed regulatory environment;
- Reflecting the industry's increasing security maturity and alignment of security expectations between stakeholders;
- Resolving unclear separation in areas where terms would describe shared responsibilities; and
- Improving clarity and structure by breaking complex clauses into separate clauses.

About HSCC CWG

[The Healthcare and Public Health Sector Coordinating Council \(HSCC\) Cybersecurity Working Group \(CWG\)](#) is a 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 develops and publishes free healthcare cybersecurity leading practices and policy recommendations, and promotes the imperative that cyber safety is patient safety. Its semi-annual All-Hands membership meetings are working sessions to strategize with government about current future health sector cybersecurity initiatives.

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