Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Industry Publishes
Model Contract Language for Medical Technology Cybersecurity

Washington, D.C., March 3, 2022 - Medical technology companies and health delivery organizations have a new template for agreeing on cybersecurity contractual terms and conditions to reduce cost, complexity and time in the contracting process and improve patient safety. Published today by the Health Sector Coordinating Council Cybersecurity Working Group (CWG) is "**Model Contract-Language for Medtech Cybersecurity (MC^2)**." This guidance was two years in the drafting process by a large and dedicated cross-sector team led jointly by Mayo Clinic and Premier Inc.

Problem

The genesis of this resource was the recognition that medical device cybersecurity responsibility and accountability between Medical Device Manufacturers (MDM's) and Health Delivery Organizations (HDO's) is complicated by many conflicting factors, including: uneven MDM capabilities and investment in cybersecurity controls built into device design and production; varying expectations for cybersecurity among HDOs; and high cybersecurity management costs in the HDO operational environment throughout the device lifecycle. These factors have introduced and sustained ambiguities in cybersecurity accountability between MDM's and HDO's that historically have been reconciled at best inconsistently in the purchase contract negotiation process, leading to downstream disputes and potential patient safety implications.

Solution

The purpose of this Model Contract Language is to offer a reference for shared cooperation and coordination between HDO's and MDM's regarding the security, compliance, management, operation, services, and security of MDM-managed medical devices, solutions, and connections. This Model Contract Language is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of HDO healthcare technologies, infrastructures, and information. This Model Contract Language articulates adequate security of HDO information being stored, transferred, or accessed and provides that all network access, medical devices, services, and solutions satisfy the mission, security, and compliance requirements of the HDO.

Medical device manufacturers, health delivery organizations, and group purchasing organizations are encouraged to closely review this contract language and adopt as much as is appropriate for the organization. The more uniformity and predictability the sector can achieve in cross enterprise cybersecurity management expectations, the greater strides it will make toward patient safety and a more secure and resilient healthcare system.

Process

This model contract is also the product of model collaboration between two subsector stakeholders whose expectations about responsibility and accountability for cybersecurity have not always been aligned. The 2-year process of "pre-negotiating" this model contract language – beginning in March 2020 - facilitated increased mutual understanding and trust between MDM's and HDO's that participated in the Medical Device Cybersecurity Model Contract Language Task Group. The sector owes the leaders and members of the task group its thanks and congratulations.

In the pipeline to be published in the coming weeks will be best practices guidance for medical device vulnerability communications to the patient audience.

Other HSCC Joint Cybersecurity Working Group resources published since 2019 include:

- **Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)**:
  HIC-STAT identifies cyber risks and best practices associated with the use of telehealth and telemedicine, and summarizes the policy and regulatory underpinnings for telehealth/telemedicine cyber risk management. It is targeted for senior executives in healthcare and IT, telehealth service and product companies, and regulators.
- **Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2)**:
  The HIC-SCRiM v2 is a toolkit for small to mid-sized healthcare institutions to manage the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program.
- **Health Sector Return-to-Work (R2W) Guidance**:
  This guidance compiles recommendations and considerations for managing a return-to-work ("R2W") strategy for our healthcare institutions and companies approaching COVID phase-down, both domestically and internationally.
- **Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)**:
  The HIC-TCR is a tactical guide to advise health providers on tactical response activities for managing the cybersecurity threats that can occur during an emergency, such as the COVID-19 Pandemic.
- **Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)**:
  The HIC-PIC is a white paper with guidance for how healthcare organizations can protect trade secrets, medical research and other innovation capital from cyber theft.
- **Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP)**:
  The HIC-ISBP is a best practice guide for how healthcare organizations can set up and manage cyber threat information sharing programs for their enterprise.
- **Management Checklist for Teleworking Surge During COVID-19 Response**:
  The Teleworking Management Checklist is designed as a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and I.T. security, and supply chain resilience.
- **Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)**:
  The HIC-MISO identifies many of the cybersecurity information sharing organizations and their key services, as health organizations are beginning to understand the importance of cybersecurity information sharing and implementing information sharing systems.
- **Health Industry Cybersecurity Workforce Guide**:
  The HIC Workforce Guide is a tool kit for recruiting and retaining skilled cybersecurity workforce in the healthcare sector.

- **Health Industry Cybersecurity Practices (HICP)**:
  The HICP is a four-volume publication that seeks to raise awareness on managing cyberthreats and safeguarding patient safety for executives, health care practitioners, providers, and health delivery organizations, such as hospitals.
- **Medical Device and Health IT Joint Security Plan (JSP)**:
  The JSP is a total product lifecycle reference guide to developing, deploying and supporting cyber secure technology solutions in the health care environment.

About the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG). The HSCC is an industry-driven advisory council of health companies and providers developing collaborative solutions to mitigate threats to critical healthcare infrastructure. It is one of 16 critical infrastructure sectors organized to partner with the government under Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. The HSCC Cybersecurity Working Group (CWG) includes more than 300 health providers entities, medical device and health IT companies, plans and payers, labs, blood and pharmaceutical companies, public health and several government partners.

For more information: Greg Garcia, HSCC Cybersecurity Working Group Executive Director: Greg.Garcia@HealthSectorCouncil.org or visit us online at https://healthsectorcouncil.org

##