Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY

MODEL CONTRACT LANGUAGE FOR MEDTECH CYBERSECURITY (MC^2)

FREQUENTLY ASKED QUESTIONS

What is the purpose of the model contract language?

The purpose of this Model Contract Language is to offer a reference point for shared cooperation and coordination between the Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) regarding the security, compliance, management, operation, services, and security of MDM managed medical devices, solutions, and connections.

Who participated in the development of the model contract language?

The HSCC Model Contract Language task group is a cross sector coalition of HDO's MDM's, and Group Purchasing Organizations (GPOs) formed to address the opportunity of developing model contract language for cybersecurity terms and conditions related to medical device purchasing and deployment. The task group included some of the most influential manufacturers and healthcare delivery organizations.

What is the intended use of the model contract language?

The intended use of the Model Contract Language is to protect HDO's against cybersecurity threats and risks through establishment and maintenance of appropriate security contract terms and commitments. This Model Contract Language provides an appropriate structure to address cybersecurity provisions and establishes requirements for HDOs and MDMs to reduce the risk of exposure.

The model contract language provides a foundation for HDOs and MDMs to negotiate and define which party will be responsible for which tasks. FDA Premarket guidance recognizes that cybersecurity "is a shared responsibility among stakeholders throughout the use environment of the medical device system, including health care facilities, patients, health care providers, and manufacturers of medical devices." One benefit of the using the model contract language framework is to establish a clear understanding of who is responsible for what roles and tasks necessary to better ensure devices are securely designed and implemented and that emerging cybersecurity risks are mitigated throughout the total product lifecycle.

How will HDOs determine which of the model contract language clauses are appropriate?

HDOs should review the technologies under consideration and determine which clauses are appropriate for the risks being introduced into a clinical environment. They should determine which responsibilities will be borne by themselves and which responsibilities will be provided by the manufacturer or service provider.

How will MDMs determine which of the model contract language clauses are appropriate?

MDMs should review the technologies they are providing and determine which clauses are their responsibility to provide as determined by functionality, design, and support constraints of the technology.

What are the benefits of using the model contract language framework?

A common model contract language framework can provide the following benefits:

- Enhanced efficiencies and lower costs
- Reduced negotiation and execution times
- Improved legal and operational process compliance
- Greater alignment between contracts
- Better staff awareness and understanding
- Reduced security risk

Does the Model Contract Language favor the HDO?

Suppliers may unilaterally impose cybersecurity requirements on themselves and the HDO through "Instructions for Use", user and service manuals, technical bulletins, cybersecurity whitepapers, and other cybersecurity artifacts. The model contract language framework provides a basis for healthcare delivery organizations to strengthen clarity of mutual obligations between parties to a contract as foundations for mature cybersecurity risk management, resulting in clearer references for obligations, accountability and liability.

Will all of the Model Contract Language clauses need to be included in every contract?

No, MDMs and HDOs will negotiate and agree upon the clauses and language appropriate for the technology and services under consideration. The model contract language framework provides a foundation of potential areas which should be considered in the development of a continuous shared responsibility partnership.

Can the clause language be modified?

Yes, each entity should perform a legal review to ensure that everything is clearly and accurately stated and that your company is comfortable moving forward according to the agreed upon terms of the agreement. Each clause is categorized and written to convey purpose and intent. The contract language should be reviewed and aligned to include the appropriate security contract clauses to address cybersecurity requirements.

Is this or will this become a government requirement?

No. This is voluntary, industry-developed, suggested model contract language. Government partners did not participate in this contract development and have not indicated intention to require use of this language or to reference it any regulatory frameworks.

What process did you use to draft this model contract language? Does this have broad support in the industry?

This is a consensus document with broad support. All Health Sector Coordinating Council documents developed by the Cybersecurity Working Group follow transparent development, review and approval procedures. The task group that developed this model language consisted of 30 organizations in healthcare delivery, medical technology manufacturing, group purchasing, servicing and consulting. The drafting negotiation process was a model demonstration of collaboration and mutual understanding.

When completed, the final draft document was circulated to the entire Cybersecurity Working Group membership of 320 organizations for review and feedback. The review period lasted 2 weeks, from October 14 to October 28, 2021. 156 substantive and editorial comments were offered by 12 organizations in a share-drive feedback form for all members to see. When the comment period closed, the leadership and volunteers of the task group met weekly through the winter to adjudicate the comments. Many were accepted, others accepted with modification, and others were declined, all with notation in the feedback form about reasoning for modification or rejection. All commenters were informed of the decisions made by the task group leads and none expressed objections to content or publication. When the document was finalized and formatted it was published March 3, 2022.