



Health Sector Coordinating Council
Cybersecurity Working Group



**Secure
Medtech**

Health Industry Cybersecurity

Model Contract-Language for MedTech Cybersecurity -Version 2



NOVEMBER 2025

Table of Contents

Introduction	4
About the Health Sector Coordinating Council	5
Purpose	5
Background	6
Usage	6
Partnership Maturity Roadmap	7
Model Contract Language Framework	8
Maturity	13
Universal Coverage	13
Industry Standards Alignment	13
Security Development Lifecycle	13
Supplier Transparency	13
Current Operating System (OS) Accountability	13
Security Patch Program	13
Responsible Data Handling	13
Product Design Maturity	14
Network Controls	14
Physical Security	14
Anti-Malware	14
Audit & Logging	14
Intrusion Detection	14
Data Encryption	14
Access Management	14

Security Patching	14
Protection Against Malicious Code	14
Privilege Escalation Controls	14
Documented Reference Architecture	14
Remote Access Controls	15
Risk Reduction	15
Attack Surface Reduction	15
Secure Development	15
<i>Performance</i>	15
Vulnerability Management	15
Incident Management	15
Security Patch Validation	15
Customer Support	15
<hr/>	
Model Contract Language Template	15
<i>Document Structure</i>	15
Framework Pillar: Performance	16
Framework Pillar: Product Design Maturity	17
Signature Authority	20
<hr/>	
Next Steps / Conclusion	21
<hr/>	
Contract Clauses	22
<hr/>	
Contract Clause Definitions	47
<hr/>	
References	52
<hr/>	
Acknowledgments	53

Introduction

Cybersecurity is a critical issue for Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs), and a shared challenge. The unrelenting pace of cyber attacks has created an increasingly expensive and resource intensive environment for delivering safe and effective care. In today's partnership between HDOs and MDMs, cybersecurity requirements are often unclear, resulting in a lack of understanding and prioritization of cybersecurity best practices. For HDOs and MDMs alike, this leads to an investment in security controls that are not always aligned between stakeholders.

The 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, we first need clear alignment to existing standards, simplification of cybersecurity requirements, and scalable cybersecurity best practices for easy access and adoption. Achieving better medical product security, operational management and cybersecurity practices will require systematic maturing of these disciplines for both HDOs & MDMs, and a forum for a continuous partnership.

These best practices are finding their way into the healthcare industry, through recent Health Sector Coordinating Council (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 (MC² v.2 or "MC Squared v.2") resource is offered as an update to the original MC² published in March 2022.

MC² v.2 refinements made to the first MC² include:

- Incorporated feedback received for MC² v.1;
- Revised and expanded content to align with changed regulatory environment;
- Reflects the industry's increasing security maturity and alignment of security expectations between stakeholders;
- Resolved unclear separation in areas where terms would describe shared responsibilities;
- Improved clarity and structure by breaking complex clauses into separate clauses; and
- Corrected some mistakes.

The HSCC Cybersecurity Working Group intends to review and update this reference as experience and recommended improvements dictate. It is well understood that as technology and business agreements evolve, so must the contract language. We encourage readers who have adopted some or all of the following clauses in your contracts to share observations or recommendations that support a shared understanding about mutual

commitments related to the cybersecurity of medical product design and management. Please send your comments at any time to: ContractsFeedback@HealthSectorCouncil.org.

About the Health Sector Coordinating Council

The Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG) is an industry-led critical infrastructure advisory council recognized by the government under a national public-private partnership framework. It's almost 500 healthcare providers, life sciences, medical technology, payers, health information infrastructure entities and government agencies partner to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care.

The JCWG membership collaboratively develops and publishes free healthcare cybersecurity leading practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

For more information about joining the HSCC as a healthcare entity, please visit <https://healthsectorcouncil.org/contact/>.

Purpose

The purpose of MC² v2 is to offer a 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. 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. MC² articulates adequate security of 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 recommended language is intended to approximate the most used cybersecurity contract terms and conditions between MDMs and HDOs, but it is not comprehensive, recognizing occasional unique situations requiring additional negotiation. It is also recognized that the wording in some recommended clauses may be modified during contract negotiations. Ultimately, as model contract language that is “pre-negotiated” extensively among some of the nation’s largest MDM and HDO organizations, this resource will serve as a scalable and periodically-updated template for large, medium and small organizations.

The language in this document is not intended to provide or constitute legal advice and parties should have their contracts reviewed by legal counsel.

The HIPAA Security Rule requires healthcare providers to protect patients' electronic Protected Health Information (ePHI) by using appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of this information. Keeping patient data safe requires healthcare organizations to exercise best practices in three areas: administrative, physical security, and technical security. In addition, model contract language should help align compliance with Food and Drug Administration (FDA) safety and effectiveness

requirements as they pertain to cybersecurity. The Model Contract Language contains security and privacy agreement clauses. Both parties need to understand their responsibilities to each other in protecting the privacy and security of the healthcare medical technology systems they will connect, and the information required to service, store and transmit. In addition to assigning specific responsibilities to MDM's, the Model Contract Language outlines security safeguards, including security by design, medical product software maintenance, access, administrative, operational, technical requirements, and transparency.

Background

The HSCC CWG Model Contract Language Task Group first convened in February 2020 as a cross-sector collaboration of 50 HDOs, MDMs, security and compliance specialists, and Group Purchasing Organizations (GPOs) to develop model contract language for cybersecurity terms and conditions related to medical product purchasing and deployment. The motivation behind the task group was the recognition that inconsistent terminology and expectations in contract language between HDOs and MDMs is partly responsible for ambiguities about cybersecurity responsibility and accountability between MDMs and HDOs. After almost 2 years of task group deliberations the resulting MC² published in 2022 was, in effect, a pre-negotiated contract that would be adaptable, tailored and scalable across the spectrum of contract parties with the hope of more uniform and repeatable sets of expectations to minimize contract negotiation time, ambiguities, disagreements and costs.

Since its publication, MC² attracted approximately 1,500 downloads from HSCC CWG website, and its usage and implementation over the course of 18 months resulted in 98 feedback comments. In mid 2024 the Model Contract ask Group reconvened to review the feedback and incorporate much of what was offered as improvement into the version 2. The end result is a simplification of the contracting process - more predictable and less costly and time-consuming.

Usage

The intended use of the Model Contract Language is to protect HDO's and patients 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. If HDO cybersecurity expectations of MDMs are not clear, and risk assessments are not continually performed, risk increases significantly to an HDO.

The use of the Model Contract Language provides HDOs contract terms that can be used as a standalone agreement covering HDO cybersecurity requirements for all medical products, services, and solutions. It also can be used as an addendum to a Business Associate Agreements (BAA), Master Service Agreements (MSA), and Requests for Proposals (RFP) in case such agreement is required. The language can be updated to fit the specific compliance needs of the HDO. While the recommended language is intended to approximate the most used cybersecurity contract terms and conditions between MDMs and HDOs, it is not comprehensive, recognizing occasional unique situations requiring additional negotiation. It is also recognized that the wording in some recommended clauses may be modified during contract negotiations.

Partnership Maturity Roadmap

The Model Contract Language partnership maturity roadmap (Figure 1: Partnership Maturity Roadmap) recognizes that requirements vary by customer and technology and that requirements and capabilities may evolve over the agreement's term. The roadmap outlines three phases to guide MDMs and HDOs in aligning or realigning the contract terms as the requirements and capabilities evolve. The three phases may be applied at different intervals as requirements and capabilities mature at various paces over the life of the agreement

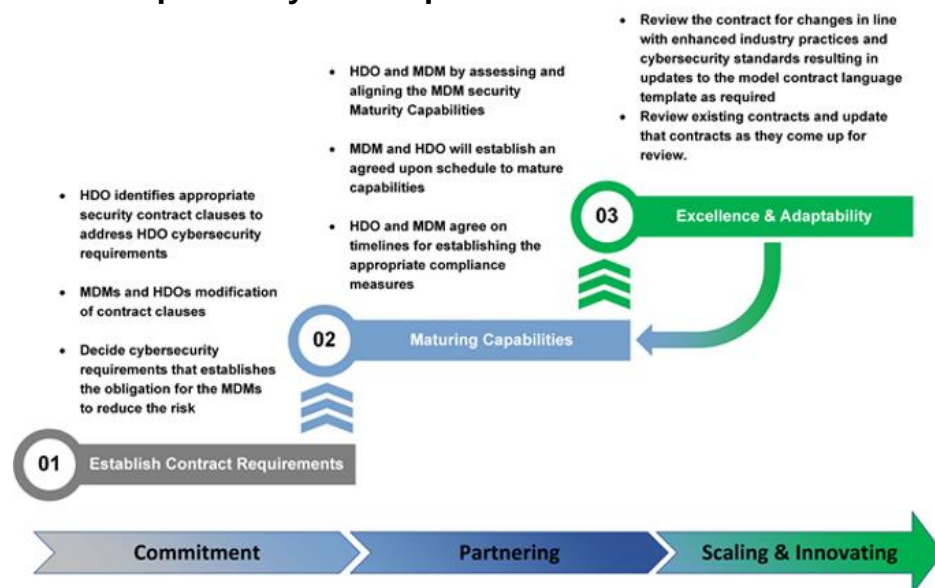
An example of this might be that federated authentication is unavailable during procurement but is on the product development roadmap for delivery within the next twenty-four months. The agreement should reflect the current capabilities or limitations, identify a mitigation development timeframe, and provide a mechanism to review and adjust the agreement at such thresholds.

In the first phase (01) of the partnership maturity roadmap, the contract language is reviewed collaboratively. The appropriate security contract cybersecurity requirements are identified and agreed upon, establishing the obligations of each party to reduce the risk of cyber threat exposure for HDOs. This phase also involves the identification of additional desired cybersecurity, enabling the collaboration and partnership of the MDMs and HDOs involved and integral to the process.

The second phase (02) of this maturity roadmap sets forth requirements that an MDM is not capable of complying with at the time of the agreement. However, the MDM and HDO will establish an agreed-upon schedule to mature capabilities, demonstrating a proactive approach to addressing future capabilities and instilling confidence in the forward-thinking nature of the agreement.

The third phase (03) sets a contract review schedule for changes in line with agreed-upon development cycles, enhanced industry practices, and cybersecurity standards and updates the model contract language as required. This may require more than one date to review specific milestones but also allows for ad-hoc reviews for unanticipated changes in standards, capacities, or capabilities.

Figure 1: Partnership Maturity Roadmap



Model Contract Language Framework

The Joint Cybersecurity Working Group developed this model contract framework and contract clauses to provide HDOs and MDMs a neutral framework for their contractual cybersecurity relationships. HDO and MDM cybersecurity experts have drafted this contract and clauses to protect the interests of healthcare from increasing cyber threats. The model contract combines a single framework of rules with flexible provisions allowing HDOs and MDMs to supplement the template with their unique requirements. Finally, it includes updates that establish a partnership arrangement between an HDO and MDM by aligning the MDM security Maturity Capabilities and HDO security requirements with the model contract language.

This model contract framework and contract clauses are designed on three fundamental cybersecurity pillars: Performance, Maturity, and Product Design Maturity. Within each of these pillars, the contract clauses are further organized into fourteen core principles, as illustrated in Figure 2: Contract Framework.

Figure 2: Contract Framework

14 Core Principles

Performance

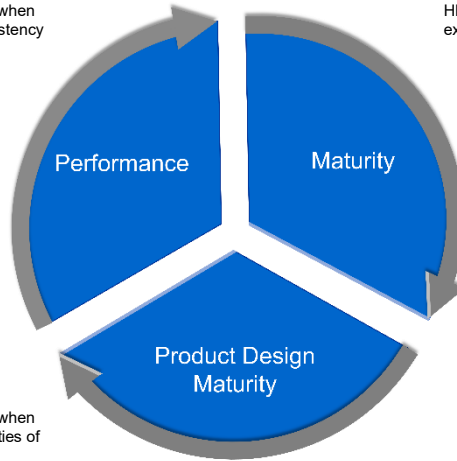
HDOs & MDMs should consider these principles when setting expectations around timeliness and consistency of support

- Vulnerability Management
- Incident Management
- Security Patch Validation
- Customer Support

Product Design Maturity

HDOs & MDMs should consider these principles when setting expectations around the inherent capabilities of the product at the time of delivery

- Secure by Design
- Standard Security Controls
- Remote Access Controls

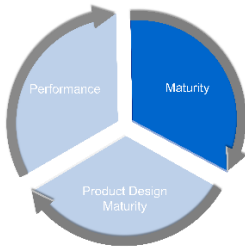


Maturity

HDOs & MDMs should consider these principles when setting expectations around capabilities, and consistent practices

- Universal Coverage
- Industry Standards Alignment
- Security Development Lifecycle
- Supplier Transparency
- Defined Security Support Lifetimes
- Security Patch Program
- Responsible Data Handling

Framework for HDO & MDM Data Security Partnership



Universal Coverage – Security requirements apply to all Customer locations, all Supplier infrastructure, and all Sub-contractors of the Supplier.

Industry Standards Alignment – Supplier demonstrates maximum adherence to industry regulations & standards, with timely adoption of new standard versions

Security Development Lifecycle – Supplier will support a program for pre-market and post-market penetration and vulnerability testing, Supplier maintains awareness of SANS top 25 and OWASP, and Supplier infrastructure is monitored 24x7

Supplier Transparency – Known vulnerabilities should be disclosed, default accounts and settings are documented, and strategic roadmaps for product/controls development are shared with the customer. Reference architectures are clearly documented.

Current OS Accountability – Supplier demonstrates accountability for validating the product on supported Operating Systems.

Security Patch Program – Supplier demonstrates accountability for validating security patches for their software and any 3rd party software on their products.

Responsible Data Handling – Good practices for storage, availability, backup, and handling of data and logs, including at the time of product disposal. Controls that enable HIPAA & other privacy requirements.

Contract Example

Reducing Attack Surface:

“Business Associate will disclose to Customer all default authentication methods or accounts, including those used for Business Associate provided maintenance and support of the device.”

Why are these principles important?

- Always: Industry Standards & Best Practice
- Indicate the values, culture, and ethos of an MDM
- Emphasize the importance of adaptability

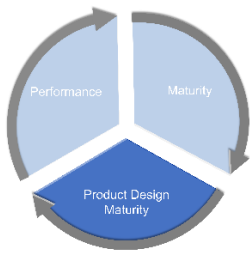
How do HDOs & MDMs partner on this?

- Dialogue at the time of new partnership between HDO & MDM
- Demonstrated through pending post-market audits & reporting from the MDM
- Ongoing dialogue about the evolving standard FDA regulations

Industry Alignment Examples:

- ✓ CIS Control #3: Continuous Vulnerability Management
- ✓ NIST SP 800-53
- ✓ CA-7, RA-4, SI-2, CA-8
- ✓ Health Sector Council Joint Security Plan

Framework for HDO & MDM Data Security Partnership



Secure by Design – A proactive approach to software and hardware development that includes security from the earliest phases of development.

Current OS Accountability – Supplier demonstrates accountability for validating product on supported Operating Systems.

Standard Security Controls – Product should have:

- Network Controls
- Physical Security
- Anti-Malware
- Audit & Logging
- Intrusion Detection
- Data Encryption
- Access Management
- Security Patching
- Protection against malicious code
- Privilege Escalation Controls
- Documented reference architecture

Remote Access Controls

Contract Example

Default Security Settings:

“Business Associate shall enable all security features for the Devices as the default setting, unless otherwise specified by the customer.”

Why are these principles important?

- Always: Industry Standards & Best Practice
- Default security reduces error opportunities
- Clear guidance indicates where to invest in controls

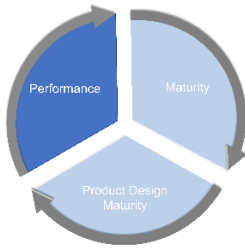
Industry Alignment Examples:

- ✓ CIS Top 20 Controls (all)
- ✓ ISO/IEC 27000
- ✓ FDA Pre- & Post-Market Cybersecurity Guidances

How do HDOs & MDMs partner on this?

- Incorporated into product evaluations and ongoing audits
- Leverage industry standard surveys & shared intelligence
- Evaluate once, share many times

Framework for HDO & MDM Data Security Partnership



Vulnerability Management – Supplier proactively discloses high risk vulnerabilities and action plans to remediate

Incident Management – Supplier actively engages during an incident and provides all necessary support to remediate in a timely manner.

Security Patch Validation – Supplier consistently validates newly released security patches for their software as well as any 3rd party software on their products.

Customer Support – Supplier consistently demonstrates secure behavior in all onsite and remote access to Customer infrastructure.

Contract Example

Communication Strategy:

“Supplier shall coordinate with Customer to identify and document a communications strategy for urgent & non-urgent engagement as it relates to vulnerability management. This strategy must at a minimum...”

Why are these principles important?

- Always: Industry Standards & Best Practice
- Threat landscape is constantly evolving
- Incidents are high risk, high visibility

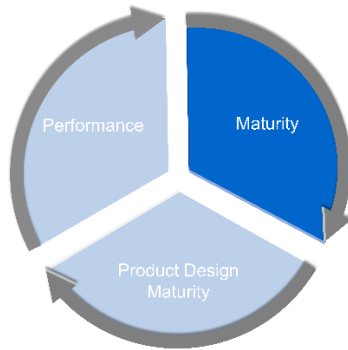
How do HDOs & MDMs partner on this?

- Dialogue about Key Performance Indicators (KPIs), which could include:
 - Service Level Agreements (SLAs)
 - How Success is defined and demonstrated
 - Roles & responsibilities for both the HDO and the MDM
 - Penalties of incentives for performance against KPTs
- Performance should be reviewed regularly

Industry Alignment Examples:

- ✓ NIST SP 800-53
- ✓ IR-5, IR-8
- ✓ ISO 29147 & ISO 30111
- ✓ Health Sector Council Joint Security Plan

Maturity



The Program Maturity pillar of the Collaborative Framework for HDO & MDM Data Security Partnership provides guidelines for the expectations, behaviors, and consistent practices for both HDOs and MDMs.

Universal Coverage – Security requirements apply to all Customer locations, all Supplier infrastructure, and all Sub-contractors of the Supplier.

Industry Standards Alignment – Supplier demonstrates maximum adherence to industry regulations & standards, with timely adoption of new standards versions.

Security Development Lifecycle – Supplier will implement security lifecycle processes in compliance with industry practices and regulatory requirements.

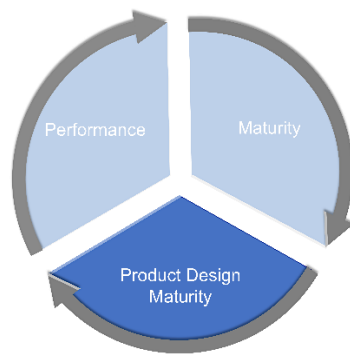
Supplier Transparency – Supplier will ensure that expectations with customers and partners are appropriately set and fulfilled and demonstrate open communication with stakeholders about matters related to the business.

Current Operating System (OS) Accountability – Supplier demonstrates accountability for validating product on supported Operating Systems.

Security Patch Program – Supplier demonstrates accountability for validating security patches for their software and any 3rd party software on their products.

Responsible Data Handling – Good practices for storage, availability, backup, and handling of data and logs, including at the time of product disposal. Controls that enable HIPAA & other privacy requirements.

Product Design Maturity



HDOs & MDMs should consider these principles - Security by Default, Standard Security Controls, and Remote Access Controls - when setting expectations around the inherent capabilities of the product at the time of delivery.

Network Controls - are used to ensure the confidentiality, integrity, and availability of the network services. These security controls are either technical or administrative safeguards implemented to minimize the security risk.

Physical Security - is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage.

Anti-Malware- Anti-malware is a type of software developed to scan, identify and eliminate malware, also known as malicious software, from an infected system or network.

Audit & Logging - Audit logs are records of event logs, typically regarding a sequence of activities or a specific activity.

Intrusion Detection - is a product or software application that monitors a network or host for malicious activity or policy violations.

Data Encryption - is a way of translating data from plaintext (unencrypted) to ciphertext (encrypted) for the purpose of protecting information confidentiality and integrity at rest and in transit

Access Management - is a system used to manage the access of resources by employees, partners, contractors and customers.

Security Patching - software that a company issues whenever a security flaw is uncovered.

Protection Against Malicious Code - protection mechanisms include antivirus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code

Privilege Escalation Controls - controls that limit illicit access of elevated rights, or privileges, beyond what is intended or entitled for a user.

Documented Reference Architecture - the essentials of existing architectures, taking into account future needs and opportunities, ranging from specific technologies to patterns to business models and market segments.

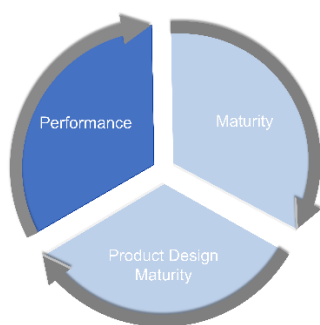
Remote Access Controls – The process of lowering the likelihood and/or impact of potential threats to an acceptable level through the implementation of security controls, mitigations, or design changes.

Risk Reduction – The ability to control and monitor access to another computer or network that isn't in your physical presence.

Attack Surface Reduction – Reducing or minimizing the set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.

Secure Development – A structured approach to designing, coding, testing and maintaining medical devices that integrates security best practices and risk management throughout the product lifecycle.

Performance



HDOs & MDMs should consider these Vulnerability Management principles when setting expectations around timeliness and consistency of support.

Vulnerability Management – Supplier proactively discloses high risk Vulnerabilities and action plans to remediate.

Incident Management - Supplier actively engages during an incident and provides all necessary support to remediate it in a timely manner.

Security Patch Validation – Supplier consistently validates newly released security patches for their software as well as any 3rd party software on their products.

Customer Support - Supplier consistently demonstrates secure behavior in all onsite and remote access to Customer infrastructure.

Model Contract Language Template

Document Structure

This Model Contract framework provides the recommended requirements to address the security safeguards within each Pillar and categorizes each recommended Clause to address each of the Core Principles within the Pillar.

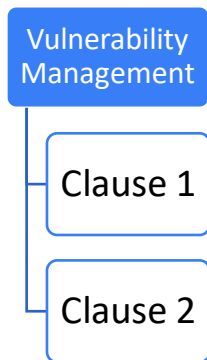
Framework Pillar: Performance

The Performance Pillar will address the recommended approach for setting expectations around timeliness and consistency of support.

The clauses under the Performance Pillar will address the following Core Principles:

- Vulnerability Management

Recommended Clause by Core Principle:



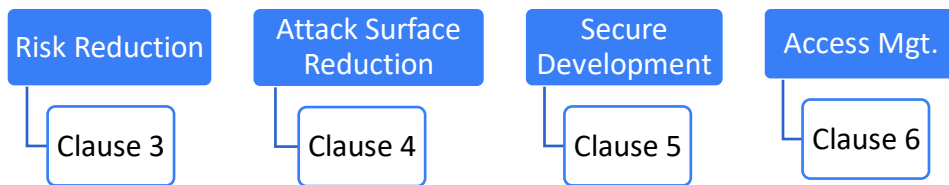
Framework Pillar: Product Design Maturity

The Product Design Maturity Pillar will address Secure by Design, Standard Security Controls and Access Controls for setting expectations around the inherent capabilities of the product.

The clauses under **Secure by Design** will address the following Core Principles:

- Risk Reduction
- Attack Surface Reduction
- Secure Development
- Access Management

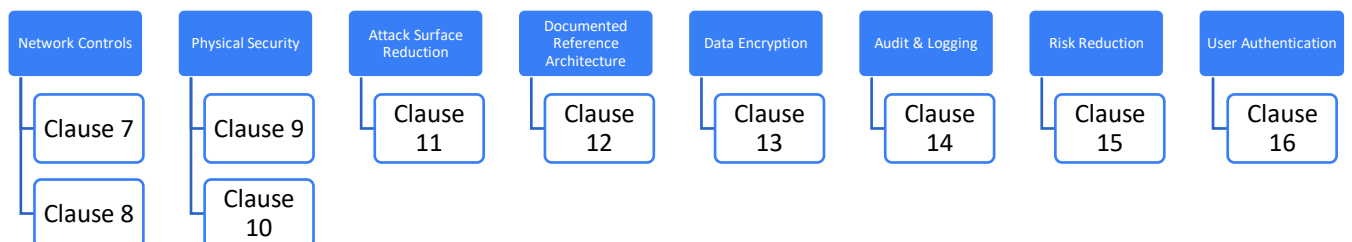
Recommended Clause by Core Principle:



The clauses under **Standard Security Controls** will address the following Core Principles:

- Network Controls
- Physical Security
- Attack Surface Reduction
- Documented Reference Architecture
- Data Encryption
- Audit & Logging
- Risk Reduction
- User Authentication

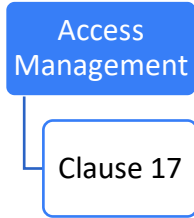
Recommended Clause by Core Principle:



The clauses under **Remote Access Controls** will address the following Core Principles:

- Remote Access Control

Recommended Clause by Core Principle:

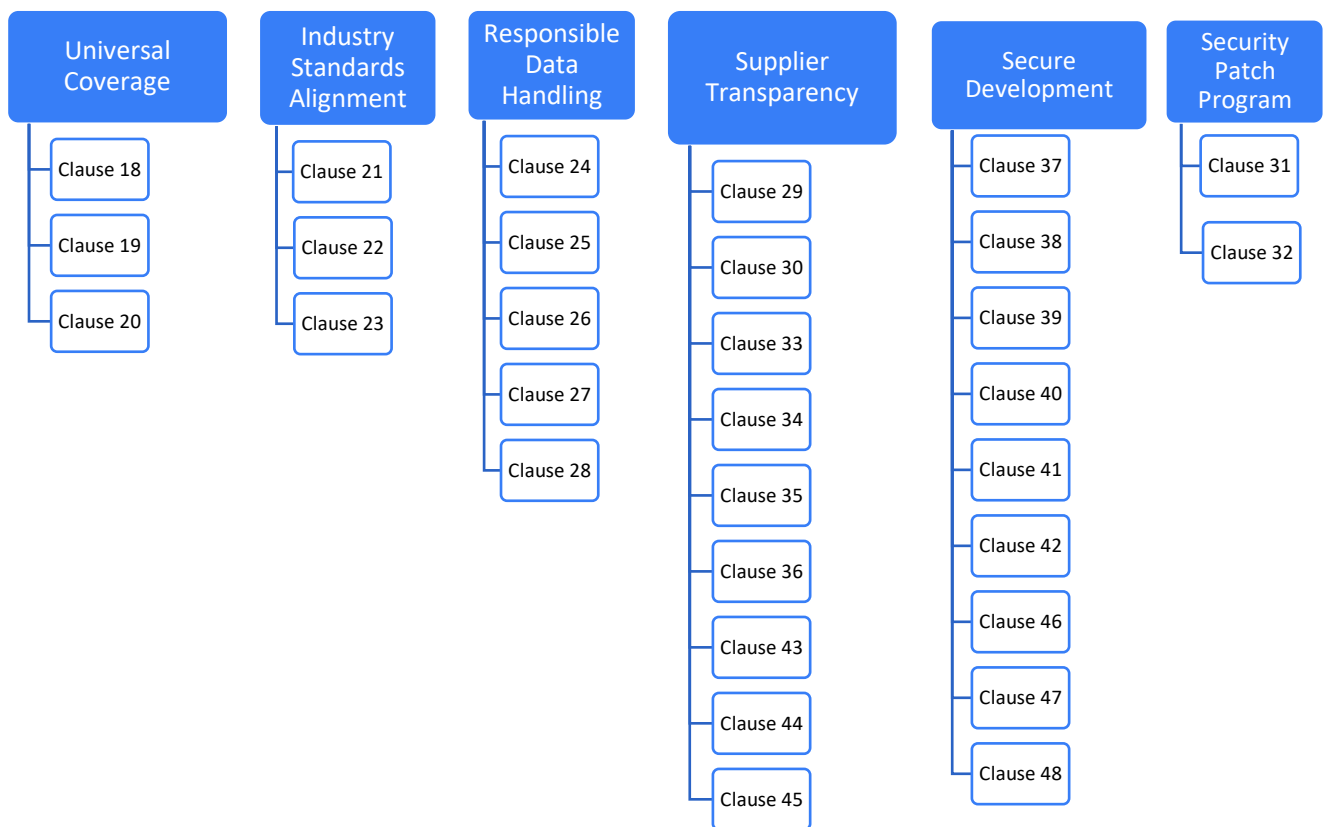


The Maturity Pillar provides guidelines for the expectations, behaviors, and consistent practices.

The clauses under **Maturity** will address the following Core Principles:

- Universal Coverage
- Industry Standards Alignment
- Security Development Lifecycle
- Responsible Data Handling
- Supplier Transparency
- Security Patch Program

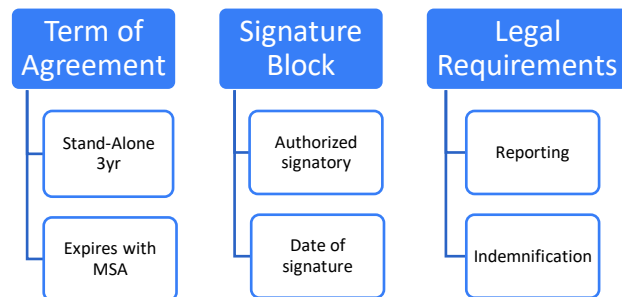
Recommended Clause by Core Principle:



Signature Authority

This optional section will indicate the term of the Agreement and the designated signatories required for each party. This section may also include additional legal statements required under the term of the Agreement (Report, Indemnification)

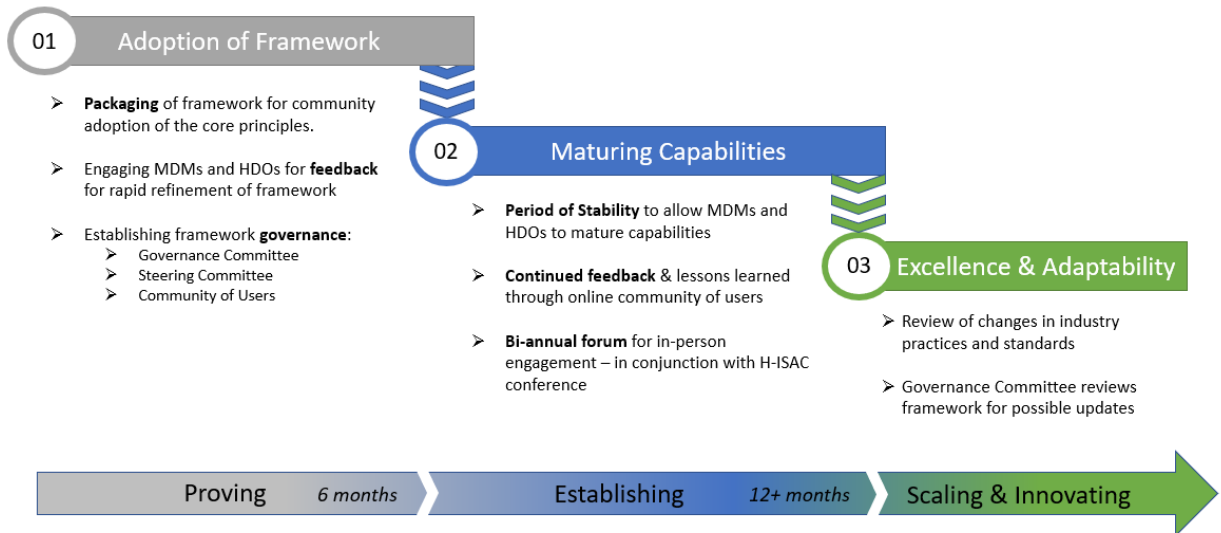
- Indicates term of Agreement
- Signature block & date
- Additional legal requirements



Next Steps / Conclusion

Figure 3: Model Contract Maturity Roadmap

The model contract maturity roadmap is a framework that describes a disciplined process focused on continuous improvement of the contract clauses.



- Adoption of Contract Model Language Framework
 - Engaging MDMs and HDOs for feedback for rapid refinement of framework and the packaging of the contract model language for community adoption of the core principles.
- Maturing Capabilities
 - A Period of Stability to allow MDMs and HDOs to mature capabilities, requiring commitments, timelines, continued feedback & lessons learned.
- Excellence & Adaptability
 - Continuous review of changes in industry practices and standards and established assurance governance, and reviews for possible updates.

Contract Clauses

Clause ID #1: Incident Responsibility	
<u>Framework Pillar:</u> Performance	<u>Core Principle:</u> Vulnerability Management
<p>Supplier shall be responsible for the costs associated with notification of affected individuals and the provision of any required consumer remedies. This can include credit monitoring or ID theft insurance for any Security Incident that arises at a Service Location and/or within the Customer’s internal network or that is associated with the Supplier’s or a Supplier subcontractor’s system or network or the Secure Services, and was caused by: (a) Supplier’s failure to perform its obligations under this Agreement or applicable Business Associate Agreement, including violations of any data security or privacy law; (b) negligent acts, omissions, and/or intentional wrongdoing by the Supplier, any Supplier Subcontractor, or any agent or employee of the Supplier or a Supplier Subcontractor.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Renamed Clause.	October 2025

Clause ID #2: Vulnerability Management	
<u>Framework Pillar:</u> Performance	<u>Core Principle:</u> Vulnerability Management
<p>When providing patches and updates the Supplier shall notify the customer of any changes to security and privacy configuration settings. Supplier shall either: a) provide patches and updates that do not modify any Customer-configured preferences and security and privacy settings of Supplier Products, or b) notify the Customer of any patches that do or may possibly modify such preferences and settings.</p> <p>Supplier shall ensure that Products only accept patches and updates that have been validated as having passed testing by the Supplier or third-party and have been formally released by the Supplier.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Removed reference to third party Services.	October 2025

Clause ID #3: Risk Reduction for Care Delivery	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Secure by Design - Risk Reduction
For all Supplier designed Medical Products, Supplier shall implement features that protect the Product’s intended use even when the Product has been compromised by a cybersecurity incident. Supplier shall document and disclose to the Customer such features.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
<u>Renamed Core Principle to “Risk Reduction”</u>	October 2025

Clause ID #4: Attack Surface Reduction and Hardening	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Secure by Design - Attack Surface Reduction
All Supplier Product cybersecurity features shall either be enabled by default (Secure by Default) or be clearly identified as requiring initial configuration. Product documentation shall specify how to enable, configure, and use all Product cybersecurity features.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
<u>Renamed Core Principle to “Attack Surface Reduction”</u>	October 2025

Clause ID #5: Secure Development	
Framework Pillar: Product Design Maturity	Core Principle: Secure by Design - Secure Development
<p>Before Supplier-designed Products are delivered to or installed at a Customer location, the Supplier shall verify and document that such Products contain commercial anti-malware technology that reduce the likelihood of any known viruses or malware infecting the device.</p> <p>Supplier Products shall install and maintain runtime detection and response capabilities such as:</p> <ul style="list-style-type: none"> (i) An application that includes industry-standard virus and malware detection capabilities that include the quarantine of files suspected to be infected and shall be updated periodically and as needed in response to changing cyber threats. or (ii) A Host Intrusion Detection and Prevention (HIDS/HIPS) Solution (Deny / Allow List Management, i.e. ‘whitelisting’) as an alternative to an anti-virus / anti-malware application. <p>If needed, Supplier shall provide documentation and instructions for the Customer how to manage, configure (Secure by Default), and integrate any security technology on the Product.</p> <p>For Products that cannot feasibly meet the requirements in this clause, Supplier shall create and provide a roadmap to meet these requirements within two (2) years or shall provide justification why the Device’s design is not able to comply.</p>	
Revision History	
Revision Summary:	Date:
Renamed Core Principle to “Secure Development” and added Supplier documentation clarification.	October 2025

Clause ID #6: Access & Credentials	
Framework Pillar: Product Design Maturity	Core Principle: Secure by Design - Access Management
<p>Supplier shall disclose to the Customer and end-user all accounts on Products. All accounts not required for proper operation, Customer use, maintenance, or administration of the Product shall be removed before Product delivery or during installation.</p>	
Revision History	
Revision Summary:	Date:
Renamed Core Principle to “Access Management”.	October 2025

Clause ID# 7: Attack Surface Reduction & Hardening

Framework Pillar: **Product Design Maturity**

Core Principle: **Standard Security Controls – Network Controls**

Supplier shall document and deliver to the Customer that:

- (i) All Product communications capabilities are fully documented and disclosed, including protocols, ports, and services.
- (ii) All network services including protocols, ports, and services not required for Product’s use shall be disabled and/or blocked prior to or during installation. Alternatively, Supplier shall document instructions to disable and/or block network services.
- (iii) Supplier shall provide documentation to recommend additional mitigating controls when the Product’s features cannot be disabled and/or blocked.

Supplier shall harden any operating system provided in any Supplier-designed Product including but not limited to:

- (i) Removal of all software and installation media not specifically required for such Products.
- (ii) Removal or disablement of all scripts, messaging services, data, and third-party installation tools after installation.
- (iii) Disablement to the extent feasible of all physical hardware ports and drives not required for use or operation of such Products after installation.
- (iv) Documenting of all hardening installation media, tools, and processes used, and all Product features, ports, drives, software, and code that remained and was removed, disabled, and not disabled.

Revision History

Revision Summary:

Date:

Renamed Core Principle to “Network Controls”.

October 2025

Clause ID #8: Secure Development	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls – Network Controls
<p>Supplier shall provide a mechanism, system, or service to detect and prevent intrusion by unauthorized users. Such monitoring systems or services along with other security systems (e.g., firewalls, anti-virus programs or HIDS/HIPS) shall generate security logs and events and shall be staffed 24x7 by qualified security personnel. Supplier shall create, update, and follow intrusion incident response policies and procedures. In accordance with HIPAA Guidelines (45 CFR § 164.316), relevant documents shall be retained for a minimum of 6 years, or as agreed on by the parties. See also (§164.308(a)(5)(ii)(C); §164.312(b); and §164.308(a)(1)(ii)(D)).</p>	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Rephrased for clarity and identification of product expectation. And updated Core principle to include “Network Controls”	October 2025

Clause ID #9: Physical Security	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls - Physical Security
<p>Supplier shall design and implement in their Products physical security controls to prevent unauthorized access to protected data. Supplier shall create, document, and provide the Customer with the physical security recommendations and requirements for securing Products in the Customer’s environment(s). In some cases, Supplier shall work with the Customer to meet the physical security needs of their Products.</p>	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Updated core principle to include “Physical Security”	October 2025

Clause ID #10: Physical Security	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls - Physical Security
Suppliers, their sub-contractors, and their third parties shall ensure that at each Service Location, the systems used to access, process, and store Customer Sensitive Information shall be operated in an environment equipped with 24-hour onsite security and monitoring, security alarm systems, and other industry-standard measures to protect the security and integrity of the Customer Sensitive Information. Supplier shall have onsite staff on duty capable of identifying, categorizing, and responding to physical security events.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Updated core principle to include “Physical Security”	October 2025

Clause ID #11: Attack Surface Reduction & Hardening	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls – Attack Surface Reduction
Supplier shall remove or disable when removal is technically infeasible all Services that are not reasonably necessary for the Product’s intended use. Where Service disabling is not feasible, Supplier will prevent the execution of unauthorized Services (e.g., by HIDS/HIPS, or anti-virus / anti-malware software). The supplier represents and warrants that Service removal or disabling will not affect the intended use of the Products. Supplier shall provide the Customer with the documentation of all required and optional Services in an MDS2 document, the Product user manual, or supplemental documentation (e.g., software bill of materials or security guidelines)	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Replaced whitelisting with HIDS/HIPS and updated core principle to include “Attack Surface Reduction”	October 2025

Clause ID #12: Secure Design	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls – Documented Reference Architecture
<p>Supplier shall implement secure software development life cycle practices in the development, design, and architecture of Products such as National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), IEC 81001-5-1 Health Software and Health IT Systems Safety Effectiveness and Security Activities in the Product Life Cycle, and FDA Cybersecurity in Medical Products: Quality System Considerations and Content of Premarket Submissions. Other industry recognized guidance as applicable:</p> <ul style="list-style-type: none"> • AAMI SW96 • CISA Secure by Design • FDA Off The Shelf Software use in Medical Devices 	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Refined clause to better align with product design frameworks and listed known guidance for clarity. Updated core principle to include “Documented Reference Architecture”	<u>October 2025</u>

Clause ID #13: Data Protection	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls – Data Encryption
<p>Supplier shall represent and warrant that all PHI, PII, and sensitive data (“Data”) shall be encrypted both at-rest and in-transit. Data shall also be encrypted on internal Product storage, on portable media, and prior to transmission. This functionality shall be in compliance with industry encryption protocols and standards. If data cannot be protected with current encryption practices or standards, supplier shall provide documentation of their roadmap to achieve this requirement within two (2) years and/or provide documentation on how to protect the data when encryption is not possible.</p>	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
<u>“Data” further defined to be inclusive of Product and is part of the information that needs to be encrypted and removed specificity on the type for flexibility.</u>	<u>October 2025</u>

Clause ID #14: Audit Controls	
<u>Framework Pillar:</u> Product Design Maturity	<u>Core Principle:</u> Standard Security Controls – Audit & Logging
<p>For Security Controls managed by the Supplier related to systems, Services, applications, and Data that are owned, rented, leased, or shared by the Customer, Supplier shall collect, retain, and provide to the Customer logs from systems, Services, applications, network products, security products, authentication controls, and anti-virus/anti-malware. Supplier shall represent and warrant that Products can log core operational functions that include but are not limited to:</p> <ul style="list-style-type: none"> i) Authentication ii) Modifications to security rules iii) Account changes iv) Major application configuration changes v) Application failures vi) Privileged use vii) Successful and unsuccessful authentication and access attempts viii) Information requests and server responses <p>Supplier shall ensure that all log files include time/date stamps of operational events, and that the Customer shall be able to review all logged data any time after data is logged.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Grammatical edits.	October 2025

Clause ID #15: Use of Portable Media	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls – Risk Reduction
<p>Supplier shall get prior written approval from the Customer to store or maintain Customer Sensitive Information on any form of removable or transportable media including but not limited to USB flash memory, thumb drives, tape, diskettes, or optical media, and on portable products including but not limited to cell phones, computers, tablets, and endpoint products. Supplier shall ensure that when Customer Sensitive Information is stored or maintained on removable or transportable media or on portable products, Customer Sensitive Information shall be encrypted in accordance with all applicable legal and regulatory requirements, including the use of strong cryptography in accordance with current industry standards.</p>	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Removed reference to NIST 800-53A.	October 2025

Clause ID #16: User Authentication	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Standard Security Controls – Access Management
<p>Supplier shall document and disclose to the Customer procedures for authentication of users to products that apply to all hardware, OS, and application authentication. Supplier shall represent and warrant that all authentication methods were designed and implemented against industry standards. Supplier shall disclose to the Customer the functional and configuration details of all authentication features built into the Product. Supplier Products shall implement basic controls to protect against unauthorized login attempts (e.g., brute force attacks and other abusive attacks). Supplier shall represent and warrant that software, scripts, accounts, and components do not contain hardcoded passwords. Supplier shall disclose to the Customer all pre-existing accounts, such as administrative or maintenance accounts. Where feasible, Products shall require users to change local passwords upon first login. Where feasible, Products shall support a central user authentication and authorization system provided by the Customer (e.g., Lightweight Directory Access Protocol (LDAP) and Active Directory).</p> <p>When the above requirements are not currently feasible, Supplier shall create and provide the Customer with the roadmap to meet such requirements within two (2) years. When the above requirements are not feasible (e.g., product design or use limitations), Supplier shall provide a risk justification why such features were not implemented and what alternatives may exist.</p>	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Replaced design with functional and configuration.	October 2025

Clause ID# 17: Remote Access Method	
<u>Framework Pillar</u> : Product Design Maturity	<u>Core Principle</u> : Remote Access Controls – Access Management
<p>Supplier shall disclose to the Customer their standard method to remotely access products or agree to comply with the Customer’s standard method of Supplier access to the Customer’s environment that includes but is not limited to:</p> <ul style="list-style-type: none"> i. Technology or solution including the protocols, ports, encryption, and authentication that are used. ii. Management of remote users. iii. Frequency and conditions for user access. iv. Logging & Auditing of all remote access & sessions are to be made available. 	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :

Clause ID #18: General Compliance	
<u>Framework Pillar</u> : Supplier Maturity	<u>Core Principle</u> : Universal Coverage
<p>Mutually agreed upon security controls and requirements as necessary shall apply in all cases in which the Supplier provides Products and/or Services that involve accessing the Customer's location, network, provision, or support of medical Products and/or middleware where Data is accessed, collected, stored, and/or transmitted to the Supplier using any method. Mutually agreed upon security controls and requirements as necessary shall apply to any form or medium of Data that includes, but is not limited to, visual, electronic, or hard copy.</p>	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Remove reference to “Universal Coverage” due to redundancy of language and instead update for mutual acceptance by MDM and HDO	October 2025

Clause ID #19: Service Locations	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Universal Coverage
The Supplier is responsible for each of their Service Locations meeting or exceeding the terms of this Agreement, including, without limitation, the Security Controls defined in this Agreement.	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Removed cloud hosting requirements within the service location.	October 2025

Clause ID #20: Supplied Contractors	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Universal Coverage
For all Subcontractors used in the performance of Services, the Supplier is responsible for each Subcontractor’s compliance with this Agreement.	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>

Clause ID #21: Compliance with Cybersecurity Regulations	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Industry Standards Alignment
For all Medical Products, at a minimum the Supplier shall comply with all required and recommended practices set forth in the local laws and regulations that determine premarket approval and postmarket management for cybersecurity.	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Reduction in specifics for compliance to allow for updates to “most current” at the time	October 2025

Clause ID #22: Secure Design	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Industry Standards Alignment
<p>Supplier shall continually assess, categorize, maintain a list of known and emerging Vulnerabilities. Supplier shall assess risks created by Vulnerabilities based on the inherent design and implementation of the product using a formalized methodology such as the Rubric for Applying CVSS to Medical Products¹ or other mutually acceptable method</p> <p>¹https://www.mitre.org/news-insights/publication/rubric-applying-cvss-medical-devices</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Removed requirement to communicate known and emerging Vulnerabilities as it is addressed in the subsequent clause.	October 2025

Clause ID #23: Vulnerability Management	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Industry Standards Alignment
<p>Supplier shall determine and classify all Vulnerabilities applicable to its Products as either Controlled Risks or Uncontrolled Risks. Supplier shall notify the Customer of all Uncontrolled Risks within 30 days of becoming aware of a Vulnerability.</p> <p>Within two (2) days of the Supplier notifying the Customer of an Uncontrolled Risk, Supplier shall provide the Customer Vulnerability descriptions including:</p> <ul style="list-style-type: none"> a) Risk impact scoring based on accepted methodologies (e.g. CVSS) b) Risk remediation strategy and processes c) Compensating controls, the Customer can implement to mitigate the risk 	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Clarified recommended risk impact scoring methodology	October 2025

Clause ID #24: Offshoring of Customer Controlled Information	
<u>Framework Pillar</u> : Supplier Maturity	<u>Core Principle</u> : Responsible Data Handling
No Customer Sensitive Information shall be stored, processed, or maintained outside of the United States, United States territories, and Puerto Rico by the Supplier or their Subcontractors without the Customer's prior written approval. Such approval may be withheld by the Customer at their sole discretion for any reason. Approval may be subject to additional terms and conditions.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :

Clause ID #25: Data Protection	
<u>Framework Pillar</u> : Supplier Maturity	<u>Core Principle</u> : Responsible Data Handling
Supplier represents and warrants that it will maintain, and ensures its permitted third-parties will maintain, the physical security of any facilities owned, managed, licensed, or controlled by Supplier that store Product data that does not reside on the Products' end points by implementing industry best security practices at the locations where the Product data is stored in order to ensure the confidentiality, integrity, and availability of the Product data and the systems that store the Product data.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :

Clause ID #26: Data Protection	
<u>Framework Pillar</u> : Supplier Maturity	<u>Core Principle</u> : Responsible Data Handling
Supplier represents and warrants that it will only collect, store, and access the minimum Data that is necessary to perform its services. Supplier shall disclose to the Customer all Data to be collected, stored, and accessed.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :

Clause ID #27: Data Protection	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Responsible Data Handling
<p>Prior to disposal of any Products returned by or on behalf of the Customer, Supplier shall securely wipe or destroy all Customer Data consistent with industry standards, such as NIST 800-88, to ensure that no Customer Data is retrievable. Upon request of the Customer, Supplier shall provide documented confirmation of Customer Data wipe or destruction. Manufacturer shall maintain records of data destruction (“Certificate of Sanitization” per NIST 800-88 for a suggested template).</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Removed ‘or discontinued’ and introduced requirement to maintain records	October 2025

Clause ID #28: Data Protection	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Responsible Data Handling
<p>Supplier, when applicable, shall maintain backup policies and procedures of Data containing Customer Sensitive Information, image repositories, and provisioned environments. The backup storage infrastructure shall be located in physically protected, limited-access facilities within the United States and governed by the cybersecurity Controls set forth herein.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>

Clause ID #29: Attack Surface Reduction & Hardening	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Supplier Transparency
<p>Supplier shall disclose to the Customer all access accounts authentication methods, including password management, for those accounts present on Products at delivery including but not limited to those used for maintenance and support of Products. Supplier will identify all hardcoded passwords.</p> <p>Supplier shall disclose to the Customer all methods for accessing Products by bypassing any authentication mechanisms for Products including but not limited to OS-level, application-level, and hardware authentication.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Changed disclosure of the password to disclosure of the authentication method and password management. Added Supplier identifying hardcoded passwords.	October 2025

Clause ID #30: Approved Mitigations	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Supplier Transparency
<p>For all Controls that the Supplier proposes as an alternative to any requirements in this Agreement must be deemed acceptable by the Customer.</p> <p>For alternative Controls deemed by the Customer as unacceptable, the Supplier shall, in good faith, identify industry-standard alternative Controls for Customer review.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>

Clause ID #31: Vulnerability Management	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Security Patch Program
<p>Supplier shall maintain the most up to date third party security patches of all Supplier managed infrastructure used to process customer data, deliver services, and solutions, to include all Supplier employee IT equipment, network infrastructure, cloud or virtual infrastructure, and any 3rd party hosted infrastructure. Supplier shall apply security patches within 30 days of the patch release. Supplier shall have a formal tracking and plan of action process for any security patches that are not implemented. Supplier will disclose all known vulnerabilities that would have an impact on customer network, or data.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Removed products and add unresolved vulnerability disclosure	October 2025

Clause ID #32: Vulnerability Management	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Security Patch Program
<p>The Supplier warrants the Products are capable of accepting all applicable Supplier approved and released security patches. Supplier shall maintain a regular patch cadence and inform customer of patch availability. The supplier will provide patch installation instructions and coordinate all patching activities with the Customer prior to installation. The supplier will make the security patches available through a secure mechanism. If patching can only be completed by the Supplier, the Supplier will patch all applicable Products at all Service Locations within 30 days of patch release.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Replace design with warrants. Added patch cadence and patch notification. Added delivery time for supplier only applied patches.	October 2025

Clause ID #33: Vulnerability Management	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Supplier Transparency
<p>For any Supplier designed Product, Supplier shall notify the Customer of all exploitable vulnerabilities that (a) are discovered to be exploited on their Product, or (b) listed in the CISA Known Exploited Vulnerability list (KEV), within three (3) business days of discovery. Notification shall include the Supplier’s timeframe for developing a response and mitigation plans. Supplier shall create, implement, and maintain a process to record, track, and report all identified exploited vulnerabilities.</p> <p>For all confirmed exploited vulnerabilities, Supplier shall take all actions necessary to assist the Customer and its delegates in investigations of the nature and impact upon the Customer and its facilities, affiliates, and patients. When requested by the Customer, Supplier shall design and implement efforts to mitigate adverse impacts.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Updated to include exploited vulnerabilities and Known Exploited Vulnerability (KEV).	October 2025

Clause ID #34: Vulnerability Management	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Supplier Transparency
<p>Supplier shall disclose to the Customer their existing communications strategy for urgent and non-urgent engagement related to vulnerability management notifications to the mutual satisfaction of both parties. In addition, both parties shall mutually share key strategic contacts, logistics for engagement, applicable Service Level Agreements (SLAs) and other information to ensure clear communication between both parties as appropriate.</p> <p>In the absence of this communications strategy, the Supplier shall coordinate with the Customer to define and document a communications strategy for urgent and non-urgent engagement related to vulnerability management notifications in alignment to applicable law(s), regulatory Postmarket Guidance, etc.</p> <p>The content of these notifications will be mutually agreed upon by both parties following established baselines such as the MedTech Vulnerability Communications Toolkit (MVCT) published by the HSCC or other mutually acceptable baselines.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Rewritten to allow supplier to provide their communications strategy for vulnerability management and allow for mutual creation of one if absent from supplier	October 2025

Clause ID #35: Incident Management	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Supplier Transparency
<p>Supplier shall notify the Customer in writing, of any use or disclosure of Customer data that is not permitted or required by this agreement or of any security incident related to Customer data as soon as reasonably practical but in no event more than five (5) days after the Supplier has determined an actual breach of Customer data and/or impact to a Customer system, unless otherwise directed by law enforcement or precluded by applicable law.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Added exception of law enforcement discretion.	October 2025

Clause ID #36: Vulnerability Management	
<u>Framework Pillar</u> : Supplier Maturity	<u>Core Principle</u> : Supplier Transparency
Supplier shall disclose to the Customer all known impacts to the safety of individuals or potential data exposure based on any Product Vulnerability being exploited. Supplier will disclose to the customer if and how a remediation of a product Vulnerability impacts the product safety, functionality, reliability, or performance.	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :
Added reliability and made other edits.	October 2025

Clause ID# 37: Secure Design	
<u>Framework Pillar</u> : Supplier Maturity	<u>Core Principle</u> : Secure Development Lifecycle
Supplier shall represent and warrant that it performed Security Assessments of potential Product security Vulnerabilities, threats, and risks as part of Product manufacturing; and either remediates the Vulnerabilities or provides recommendations for risk mitigation. Supplier shall perform Security Assessments that are consistent with industry standards for information security including the most recent versions of the National Institute of Standards and Technology (NIST) <i>Frameworks for Improving Critical Infrastructure Cybersecurity</i> and the Open Web Application Security Project (OWASP) <i>Internet of Things Framework Assessment</i> . Supplier shall disclose the standards used for assessment. Supplier shall score the Vulnerabilities consistent with accepted methodologies (e.g. CVSS).	
Revision History	
<u>Revision Summary</u> :	<u>Date</u> :

Clause ID #38: Secure Code Design & Analysis	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Secure Development Lifecycle
<p>Supplier security practices shall contain industry-standard testing processes and tools to mitigate the security risk of all Supplier-designed Products. Supplier represents and warrants that such testing processes include tools, techniques, and practices designed to discover security Vulnerabilities in Code. Supplier represents and warrants that it shall remediate or mitigate any known or discovered findings (for example, warnings or violations) prior to the delivery of Code to the Customer, or if not resolved, provide evidence that the findings shall not affect the security, safety, effectiveness, and operation of Products for their intended use. Supplier represents and warrants that all Product software including third-party is integrated using secure coding practices as part of a software development lifecycle that includes assessing all Product software to eliminate Vulnerabilities as described in the OWASP Top 10 and the CWE/SANS Top 25 most dangerous software errors. Supplier maintains a quality assurance program for Product software that identifies and corrects potential Vulnerabilities.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Expanded testing process and scope.	October 2025

Clause ID #39: Privileged Access	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Secure Development Lifecycle
<p>Supplier shall design and/or configure each Product component to operate using the Principle of Least Privilege (PoLP), including but not limited to operating system permissions, file access, user accounts, application-to-application communications and any dependencies for application, commercial software, service, or communication processes. Supplier represents and warrants that Products isolate Code, processes, and data, from Product software that does not need to access such Code, processes, or data. Supplier shall limit the number of accounts on Supplier-designed Products that require administrative privileges to known industry best practices. Supplier shall provide protections against privilege escalation, and the capability to escape from a Supplier system/application/environment and access the Customer network unless authorized by the Customer to do so.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>

Clause ID #40: Operating System Accountability	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Secure Development Lifecycle
<p>Supplier shall identify the operating system (OS) and all software in its Products. Products must not be running any OS software within two (2) years of End of Support by an OS third-party supplier at the time of Supplier’s committed delivery to a Customer location and/or expected use. If any product is running an OS within two (2) years of obsolescence, the Supplier shall provide an update path to a non-obsolete OS, at the Supplier’s expense. The Supplier may offer an extended support agreement to defer OS replacement under conditions to be mutually agreed upon.</p> <p>For all Products currently at any Service Location, the Supplier shall verify whether the installed OS is within one (1) year of obsolescence and shall notify the Customer of an upgrade option for such Products to a supported OS. Where this requirement is not currently feasible, Supplier shall provide documentation of their roadmap to achieve these requirements within two (2) years.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Revised to include defer OS replacement.	October 2025

Clause ID #41: Periodic Security Testing Response	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Secure Development Lifecycle
<p>Supplier shall implement pre- and post-market security monitoring and signal collection of its Products including periodic security testing. If Uncontrolled Risks are identified, Supplier shall develop a remediation action plan within thirty (30) days that follows industry practices such as those contained within the FDA <i>Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions</i>, and the FDA <i>Postmarket Management of Cybersecurity in Medical Devices (or applicable other regional cybersecurity regulations)</i>.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Added clarity and updated guidance references.	October 2025

Clause ID #42: Security Testing (Hosted & Cloud Solutions)	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Secure Development Lifecycle
<p>At the request of the Customer, the Supplier or an experienced third-party of the Supplier's choosing shall perform security testing and verification of the Service Locations and the systems/applications/environments involved in the Supplier's provision of the Secure Services, which may include security Vulnerability scanning, and/or penetration testing. The Supplier shall provide documented results of such testing/scanning, including information on vulnerabilities, upon request. These documented results are subject to audit by the Customer.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Added audit provision; simplified the provision of Security Services.	October 2025

Clause ID #43: Security Assessment	
<u>Framework Pillar:</u> Supplier Maturity	<u>Core Principle:</u> Supplier Transparency
<p>Supplier will respond to Customer requests to support and contribute to Security Assessments of the Product including completing questionnaires, providing interviews, responding to information requests, and providing product security artifacts or other documentation as reasonably requested. Supplier represents and warrants that the Supplier's submitted responses are complete and accurate.</p> <p>In the event of indications of non-compliance, a security event, or in advance of Risk Transfer as defined in Clause 45-Risk Transfer.</p>	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
Reworded for clarity on supplier expectations for Security Assessments along with new definition for Security Assessments in Appendix to align with change.	October 2025

Clause ID #44: Vulnerability Management	
Framework Pillar: Supplier Maturity	Core Principle: Supplier Transparency
<p>Supplier shall provide a Software Bill of Materials (SBOM) that includes but is not limited to: Open Source Software (OSS), commercially available off the shelf software (COTS), proprietary (vendor produced) software, and other software components such as libraries, frameworks, operating systems, and communication stacks used in the Product. This is inclusive of all software components contained in a medical product system.</p> <p>An SBOM shall contain at least the minimum elements as and when defined by the FDA or other industry guidance, standard, or regulation.</p> <p>The Supplier shall use the SBOM to identify during development (premarket) and maintenance (postmarket) known vulnerabilities as identified in common vulnerability databases such as the National Vulnerability Database (NVD). Supplier shall have processes in place to assess the risk associated with the identified software component vulnerabilities and take appropriate mitigation and communication actions.</p> <p>The Supplier shall monitor the unsupported components for new and emerging vulnerabilities and notify the Customer.</p> <p>NTIA-Framing Software Component Transparency: Establishing a Common Software Bill of Materials https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf</p>	
Revision History	
Revision Summary:	Date:
New clause added in Version 2.	October 2025

Clause ID #45: Risk Transfer	
Framework Pillar: Supplier Maturity	Core Principle: Supplier Transparency
<p>Supplier will notify Customer in advance of Product lifecycle thresholds to include:</p> <ul style="list-style-type: none"> • End of Life (EoL), 24-month notice • End of Guaranteed Support (EoGS), 24-month notice • End of Support (EoS), 36-month notice • End of manufacturer provided user and maintenance training, 24-month notice. <p>The EoS notices will provide security documentation to Customer for compensating controls and mitigations.</p>	
Revision History	
Revision Summary:	Date:
Added Pillar classification and added more details around expected timeframes around product lifecycle thresholds.	October 2025

Clause ID #46: Supplier Maturity	
Framework Pillar: Supplier Maturity	Core Principle: Secure Development Lifecycle
The Supplier will attest to having implemented a secure development process in alignment with existing secure development standards such as: ANSI 62443-4-1; IEC 81001-5-1; NIST SP 800-218 (SSDF).	
Revision History	
Revision Summary:	Date:
New clause added in Version 2.	October 2025

Clause ID #47: Secure Manufacturing Environment	
Framework Pillar: Supplier Maturity	Core Principle: Secure Development Lifecycle
Supplier will provide a summary describing the controls that are in place to assure that the medical product manufacturing environment will maintain its integrity from the point of manufacturing to the point at which that product leaves the control of the manufacturer.	
References:	
<ul style="list-style-type: none"> • NISTIR 8183, “Cybersecurity Framework, Version 1.1, Manufacturing Profile”, Oct. 2020 https://csrc.nist.gov/pubs/ir/8183/r1/final • NIST NCCoE SP 1800-10, “Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector, March 2022 https://csrc.nist.gov/pubs/sp/1800/10/final • DHS, CISA, “Critical Manufacturing Sector – Cybersecurity Framework Implementation Guide“, May 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf • ENISA Industry 4.0 Cybersecurity Challenges and Recommendations https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations 	
Revision History	
Revision Summary:	Date:
New clause added in Version 2.	October 2025

Clause ID #48: Cybersecurity Principles and Practices	
Framework Pillar: Supplier Maturity	Core Principle: Secure Development Lifecycle
<p>Supplier will provide an attestation that the product complies with current and applicable cybersecurity principles and practices included in FDA pre-market cybersecurity guidance or the guidance documents of other regulatory agencies. Manufacturers shall identify which frameworks and standards they are following such as but not limited to:</p> <ul style="list-style-type: none"> • ISO/IEC 81001-5-1 - Health software and health IT systems safety, effectiveness and security - Part 5-1: Security - Activities in the product life cycle • MDCG 2019-16 - Guidance on Cybersecurity for medical Products • IMDRF, "Medical Device Cybersecurity Guide", April 2023, • IEEE, 2933-2024 - Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security” • NIST CSF 2.0 , “Framework for Improving Critical Infrastructure Cybersecurity, V2.2”, March, 2023 	
Revision History	
<u>Revision Summary:</u>	<u>Date:</u>
New clause added in Version 2.	October 2025

Contract Clause Definitions

The definitions provided below are generally harmonized with the NIST CSRC Glossary:

https://csrc.nist.gov/glossary/term/security_service

Refer to the NIST CSRC document for any cybersecurity terms which are not defined here.

Agreement This contract document.

Business Associate Agreement (BAA)

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI (Protected Health Information) on behalf of, or provides services to, a covered entity. A member of the covered entity’s workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of PHI. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>

Code Executable software including but not limited to firmware, patches, updates, upgrades, and/or releases.

Control Any method to mitigate the security risk levels of Products.

Controlled Risk As defined by FDA: [Postmarket Management of Cybersecurity in Medical Devices](#) “Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a product’s particular cybersecurity Vulnerability”.

Customer Medical corporation and its business lines, employees, and patients that uses Products provided by the Supplier.

Customer Sensitive Information

Any sensitive, confidential, proprietary or other non-public information related to the business of Customer, including but not limited to: (a) all personally identifiable information, data or records relating to or concerning any patient, member, plan participant, employee or contractor of any Customer entity, including, without limitation, Protected Health Information under the Health Insurance Portability and Accountability Act (HIPAA), (b) any other sensitive information of Customer, including but not limited to: business strategy information; marketing plans; price data; non-public financial, operational or facilities information or records; information relating to or lists of actual or potential vendors, customers, Supplier, employees, independent contractors, health plan subscribers or beneficiaries, and other third parties; claims data; clinical trial results; proprietary software, hardware and other information technology of Customer's; network and security system designs, architecture, operations and configurations; and network architecture. Customer Sensitive Information shall always be Confidential Information of Customer

Cybersecurity Event A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)

Data Any form of information including but not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), electronic PHI (ePHI), sensor readings, configuration settings, authentication credentials, log files, and cryptographic keys.

Defense in Depth A concept in which multiple layers of security controls (defense) are placed throughout an I.T. system. Its intent is to provide redundancy in the event a security control fails, or a Vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical security for the duration of the system's life cycle.

Device Type of Product primarily operated by a Customer end-user.

Device Data Any Data that is collected by, transmitted to or from, or stored on a Device.

End of Guaranteed Support (EOGS)

Point after which the manufacturer no longer guarantees full support. Note: During this life-cycle stage, there can be some level of support available by the manufacturer, but without a guarantee that the medical product can be maintained to its original specification and performance. Disclaimer: This term is not identified as one of the IMDRF lifecycle stages. SOURCE: AAMI TIR97:2019

End of Life (EOL) Life cycle stage of a product, starting when (1) the manufacturer no longer sells the product beyond its useful life (as defined by the manufacturer), and (2) the product has gone through a formal EOL process, including notification to users. SOURCE: IMDRF Principles and Practices for Medical Device Security:2019

End of Support (EOS) Point after which the manufacturer has terminated all service support activities. Note: Service support does not extend beyond this point. SOURCE: AAMI TIR97:2019

Fail Safe Fail-Safe' refers to the ability of a Product to operate during and after a cybersecurity incident including but not limited to the ability to continue to function if disconnected or not connected to a network.

Host Intrusion Detection and Prevention (HIDS/HIPS) Solution

Host Intrusion Detection and Prevention system is a security technology secures a system via a deny/allow list that controls execution of processes and services (formerly known as whitelisting).

Known Exploited Vulnerability

Subset of known vulnerabilities that have been actively exploited in the wild.

Master Services Agreement (MSA)

A contractual document that outlines the general terms and conditions governing the relationship between a service provider and a client. It serves as a foundational agreement that sets the framework for future, more specific service agreements or statements of work (SOW). Within an MSA, you typically find provisions related to pricing, payment terms, intellectual property, confidentiality, dispute resolution, and other key terms that apply to all services provided by the service provider. When specific projects or services are required, the parties can refer to the MSA

and create SOWs that detail the scope, timeline, and other project-specific information.

MDS2 Manufacturer Disclosure Statement for Medical Device Security

Medical Device As defined by the FDA: [How to Determine if Your Product is a Medical Device](#).

Non-medical Device A device that is not a regulated Medical Device.

Patch A “repair job” for a piece of programming; also known as a “fix

Product Device, Service, or Solution provided by the Supplier to the Customer.

Principle of Least Privilege (PoLP)

A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks

Protected Health Information (PHI)

Defined under the HIPAA Privacy Rule as any "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

Request for Proposal (RFP)

A formal document that an organization, business, or government agency uses to solicit proposals from qualified vendors or service providers. The primary purpose of an RFP is to outline the specific needs, requirements, and expectations of the project or contract and to invite potential suppliers to submit their proposals for fulfilling those needs.

Requirement	Statement in this Agreement that the Supplier must meet.
Services	Supplier's responsibility as defined in a contractual obligation.
Security Assessment	Any method of evaluation of security risk levels of Products by customer using current Industry Standard artifacts such as NEMA's MDS2
Security Control	The definitions provided below are generally harmonized with the NIST CSRC Glossary and the U.S. CERT's NICCS Glossary .
Security Incident	The definitions provided below are generally harmonized with the NIST CSRC Glossary (https://csrc.nist.gov/glossary) and the U.S. CERT's NICCS Glossary
Sensitive Information	Data that contains Personally Identifiable Information (PII), Patient Health Information (PHI), and/or electronic Patient Health Information (ePHI).
Service	Delivery of Product security support including but not limited to cybersecurity activity monitoring, remote personnel, and hosting of data.
Service Location	Business unit of the Supplier or its Subcontractor that provides or supports Services to support this Agreement.
Shall	Reserved word that means 'must' *If no conditions are stated, 'shall' means 'must in all situations.' *If conditions are stated, 'shall' means 'must when the stated situations apply.'
Subcontractor	Contractor hired by the Supplier to meet Supplier requirements.
Supplier	A manufacturer or their representative (such as a vendor or a business associate) that provides Products to the Customer.

Uncontrolled Risk	"As defined by FDA Postmarket Management of Cybersecurity in Medical Devices https://www.fda.gov/files/medical devices/published/Postmarket-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf : Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations.
Update	Corrective, preventative, adaptive, or perfective modifications made to software of a medical product (FDA guidance).
Vulnerability	A weakness in an information system, system security procedure(s), internal control(s), human behavior, or implementation that could be exploited (FDA pre-market guidance).

References

- <https://www.fda.gov/files/medical%20devices/published/Postmarket-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf>
- <https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device>
- <https://niccs.us-cert.gov/about-niccs/glossary>
- <https://www.fda.gov/files/medical%20devices/published/Postmarket-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf>
- https://csrc.nist.gov/glossary/term/interconnection_security_agreement

It is well understood that as technology and business agreements evolve, so must contract language. The HSCC Cybersecurity Working Group intends to review and update this reference as experience and recommended improvements dictate.

We encourage readers who have adopted some or all the following clauses in your contracts to share observations or recommendations that support a shared understanding about mutual commitments related to the cybersecurity of medical product design and management.

Please send your feedback/comments/suggestions at any time to: ContractsFeedback@HealthSectorCouncil.org.

Acknowledgments

The Health Sector Coordinating Council Cyber Security Working Group wishes to express its gratitude to the many member representatives who worked on the Model Contracts Task Group and contributed significant hours and thought leadership to the development of this resource.

In particular for the October 2025 update, we wish to thank:

Michelle Bentley (Co-Chair)

Mayo Clinic

Jason Ferri (Co-Chair)

Premier

Andrew Sargent

Spacelabs

Axel Wirth

Medcrypt

Brandyn Blunt

Cleveland Clinic

Brindusa Curcaneanu

Nevro

Christopher Gates

arsMedSecurity

David Pinto

Medtronic

Emily Holmquist

Accuray

Mike Powers

St. Luke's University Health Network

Phil Englert

Health-ISAC

Terri Duket

GE Healthcare