Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY -

Model Contract-language for Medtech Cybersecurity

March 2022

Table of Contents

Introduction

Cybersecurity is not a new issue for Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs). The unrelenting pace of cyber threats 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 murky investment in controls.

The understanding and management of medical device 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 device design and production; varying expectations for cybersecurity among HDOs; and high cybersecurity management costs in the HDO operational environment throughout the device lifecycle. These factors have introduced and sustained ambiguities in cybersecurity accountability between MDM's and HDO's that historically have been reconciled at best inconsistently in the purchase contract negotiation process, leading to downstream disputes.

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 device 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) publications such as the Health Industry Cybersecurity Practices (HICP) for healthcare providers and the Medical Device and Health IT Joint Security Plan (JSP) 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 model contract language resource is offered.

It is well understood that as technology and business agreements evolve, so to must contract language. The HSCC intends to review and update this reference as experience and recommended improvements dictate. 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 device design and management. Please send your comments at any time to: ContractsFeedback@HealthSectorCouncil.org.

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 300 industry organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

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

Purpose

The purpose of this Model Contract Language 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, services, and security of MDM managed medical devices, solutions, and connections. This Model Contract Language is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of HDO healthcare technologies, infrastructures, and information. This Model Contract Language articulates adequate security of HDO information being stored, transferred, or accessed and provides that all network access, medical devices, services, and solutions satisfy the mission, security, and compliance requirements of the HDO.

This recommended language is intended to approximate the most commonly 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, the Health Sector Coordinating Council believes that, as model contract language "pre-negotiated" extensively over 18 months among some of the nation's largest MDM and HDO organizations, this resource will serve as a scalable template for large, medium and small organizations.

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 security of this information. Keeping patient data safe requires healthcare organizations to exercise best practices in three areas: administrative, physical security, and technical security. The HIPAA security rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

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 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 device software maintenance, access, administrative, operational, technical requirements, and transparency.

Background

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 intent was, in effect, to pre-negotiate complex elements of a 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.

This initiative began when a forward-thinking coalition of HDO's lead by Mayo Clinic, Cleveland Clinic, Kaiser Permanente, and Froedtert had earlier formed the "Unified Medical Device Security Alliance" to develop Model Contract Language from the HDO perspective. This former HDO alliance had made considerable progress toward developing such a framework and sought to leverage the expertise and collaboration of additional stakeholders in the MDM and group purchasing organization (GPO) communities, establishing a cross-sector collaborative process. Accordingly, after a series of discussions with the Alliance, in March 2020 the HSCC Cybersecurity Working formally integrated the Alliance's work-in-progress into a new Model Contract Language Task Group, co-led by Mayo Clinic, Siemens Healthineers, and Premier, Inc.

The Figure Boxes below identify the original HDO framework using the HDO names abbreviated as "CC/FH/KP/MC Framework for HDO & MDM Data Security Partnership"

The motivation behind the task group was the recognition that inconsistent terminology and expectations in contract language between HDO's and MDM's is partly responsible for ambiguities about cybersecurity responsibility and accountability between MDM's and HDOs. A recommended solution is the creation of a reference for the most commonly agreed-upon contract language for medical device cybersecurity, negotiated collaboratively as a template among HDO's, MDM's, and Group Purchasing Organizations (GPO's). Such a reference is intended to simplify the contracting process and make it more predictable and less costly and time-consuming. It is acknowledged that such a common reference cannot adequately cover all issues. Some unique issues to the contracting parties or types of procurement would require separate negotiation.

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. Suppliers represent one of the highest risks to HDO's for the medical devices, solutions, and connections they provide and support. 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 HDO’s contract terms that can be used as a standalone agreement covering HDO cybersecurity requirements for all medical devices, services, and solutions. It also can be used as an addendum to a Business Associate Agreement (BAA), Master Service Agreement (MSA), and Requests for Proposals (RFP).

The BAA is a legal contract that describes how the MDM adheres to the Health Information Portability Accountability Act (HIPAA) along with the responsibilities for protecting electronic Protected Health Information (ePHI). The purpose of an MSA is to set the boundaries of the contractual relationship, establishing the commitments for accomplishing the work or services that need to be done, and to provide acceptance for termination, and agreements to resolve any disputes, which may arise during the course of the service. A request for proposal (RFP) is a document that solicits proposal, often made through a bidding process.

The Model Contract Language presents a primary point for a contract covering the key areas of security. The language can be updated to fit the specific compliance needs of the HDO. This recommended language is intended to approximate the most commonly 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, the Health Sector Coordinating Council believes that, as model contract language “pre-negotiated” extensively over 18 months among some of the nation’s largest MDM and HDO organizations, this resource will serve as a scalable template for large, medium and small organizations.

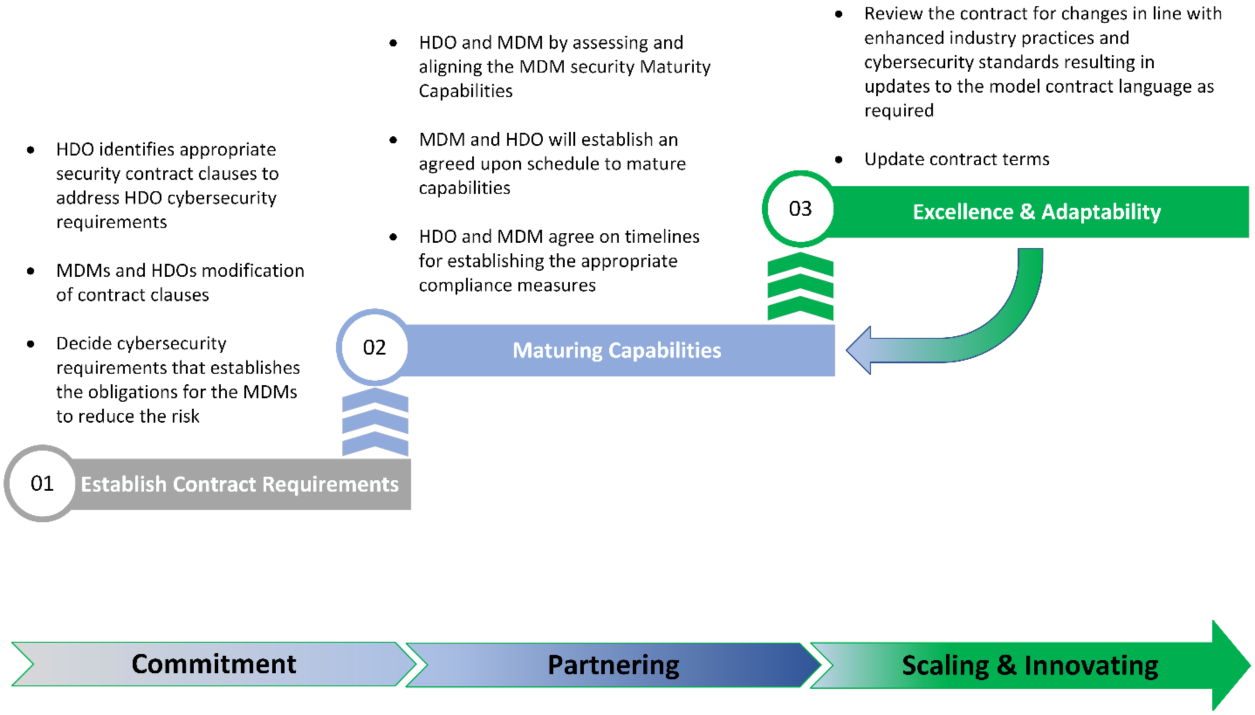
Partnership Maturity Roadmap

The model contract language partnership maturity roadmap (Figure 1: Partnership Maturity Roadmap), begins with the (01) review and alignment of the contract language and the appropriate security contract clauses to address cybersecurity requirements that establish the obligations for MDM’s to reduce the risk of cyber threat exposure for HDO’s.

The second phase (02) of this maturity roadmap sets forth the relationship between the model contract language and any HDO technologically advanced to establish future security requirements to the model contract language. If there are HDO requirements that an MDM is not capable of complying with at the time of the agreement, the MDM and HDO will establish an agreed-upon schedule to mature capabilities.

The third phase (03) is to set a contract review schedule that reviews the contract for changes in line with enhanced industry practices and cybersecurity standards and updates the model contract language as required.

Figure 1: Partnership Maturity Roadmap



- HDO identifies appropriate security contract clauses to address HDO cybersecurity requirements
- MDMs and HDOs modification of contract clauses
- Decide cybersecurity requirements that establishes the obligations for the MDMs to reduce the risk

- HDO and MDM by assessing and aligning the MDM security Maturity Capabilities
- MDM and HDO will establish an agreed upon schedule to mature capabilities
- HDO and MDM agree on timelines for establishing the appropriate compliance measures

- Review the contract for changes in line with enhanced industry practices and cybersecurity standards resulting in updates to the model contract language as required
- Update contract terms

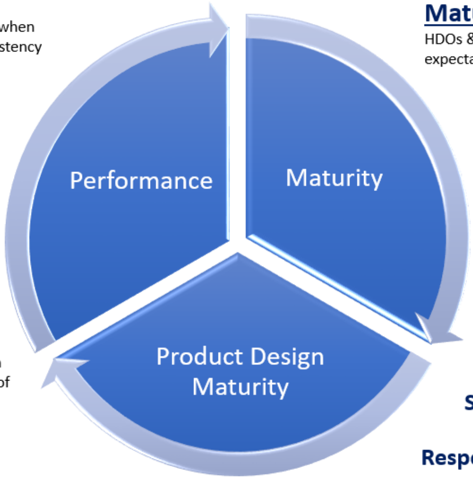
Model Contract Language Framework

The Joint Cybersecurity Working Group developed this model contract framework and contract clauses to provide HDO's and MDM's 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 HDO's and MDM's 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**

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

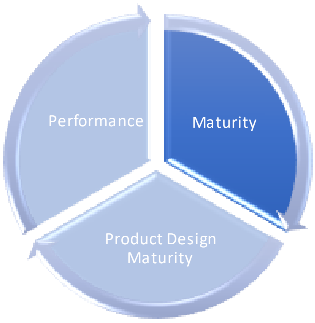
- **Universal Coverage**
- **Industry Standards Alignment**
- **Security Development Lifecycle**
- **Supplier Transparency**
- **Defined Security Support Lifetimes (e.g., Current OS Accountability)**
- **Security Patch Program**
- **Responsible Data Handling**

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 Default**
- **Standard Security Controls**
- **Remote Access Controls**

Framework for HDO & MDM Data Security Partnership

The Bar of Goodness



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 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 customer, reference architectures are clearly documented.

Current 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.

Contract Example

Reducing Attack Surface:

"Business Associate will disclose to Customer all default (non-customer) authentication methods or accounts, including those used for Business Associate provided maintenance and support or 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

Industry Alignment Examples:

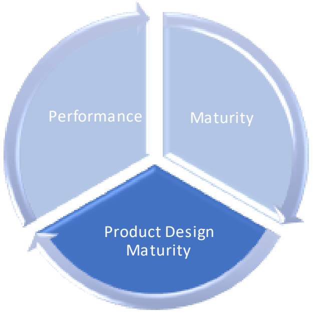
- ✓ CIS Control #3: Continuous Vulnerability Management
- ✓ NIST SP 800-53
  - ✓ CA-7, RA-4, SI-2, CA-8
- ✓ Health Sector Council Joint Security Plan

How do HDOs & MDMs partner on this?

- Dialogue at the time of new partnership between HDO & MDM
- Demonstrated through pre- and post-market audits & reporting from MDM
- Ongoing dialogue about evolving standards (e.g. FDA Regulations)

Framework for HDO & MDM Data Security Partnership

The Bar of Goodness



Secure by Default– Product should by default have all security features enabled, attack surfaces are reduced, and should be free of malware or unnecessary code and services.

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 customer."

Why are these principles important?

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

How do HDOs & MDMs partner on this?

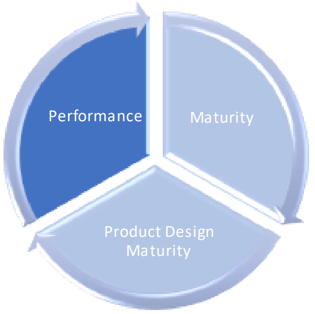
- Incorporated into product evaluations and ongoing audits
- Leverage industry standard surveys & shared intelligence
  - Evaluate once, share many times

Industry Alignment Examples:

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

Framework for HDO & MDM Data Security Partnership

The Bar of Goodness



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

Incident Mgmt. – Supplier actively engages during an incident and provide 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

Industry Alignment Examples:

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

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 HDO and MDM
  - Penalties of incentives for performance against KPIs
- Performance should be reviewed regularly

Model Contract Library

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.

Maturity

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 support a program for pre-market and post-market penetration and vulnerability testing; for instance, Supplier maintains awareness of SANS top 25 and OWASP, and Supplier infrastructure is monitored 24x7.

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 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 these event logs, typically regarding a sequence of activities or a specific activity.

Intrusion Detection - is a device 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).

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

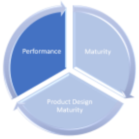
Security Patching - software that a company issues whenever a security flaw is uncovered.

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



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 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.

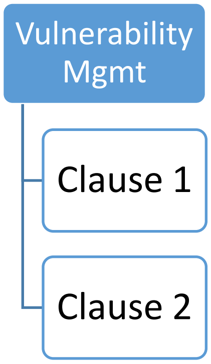
Framework Pillar: Performance

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:



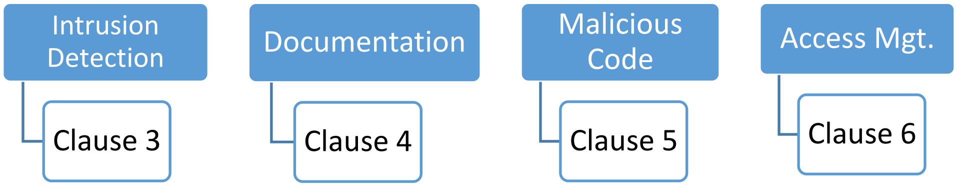
Framework Pillar: Product Design Maturity

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

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

- Intrusion Detection
- Documented reference architecture
- Protection against malicious code
- Access Management

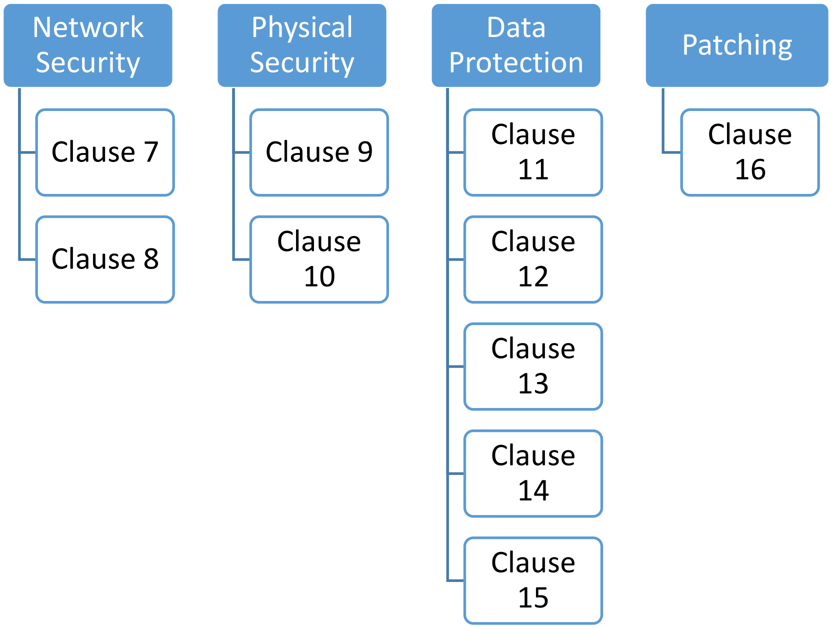
Recommended Clause by Core Principle:



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

- Network Controls
- Physical Security
- Data Protection including Anti-Malware, Audit & Logging, Data Encryption and Privilege Escalation Controls
- Security Patching

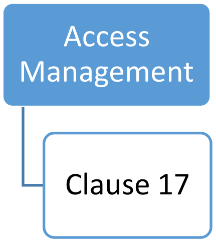
Recommended Clause by Core Principle:



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

- Access Controls

Recommended Clause by Core Principle:



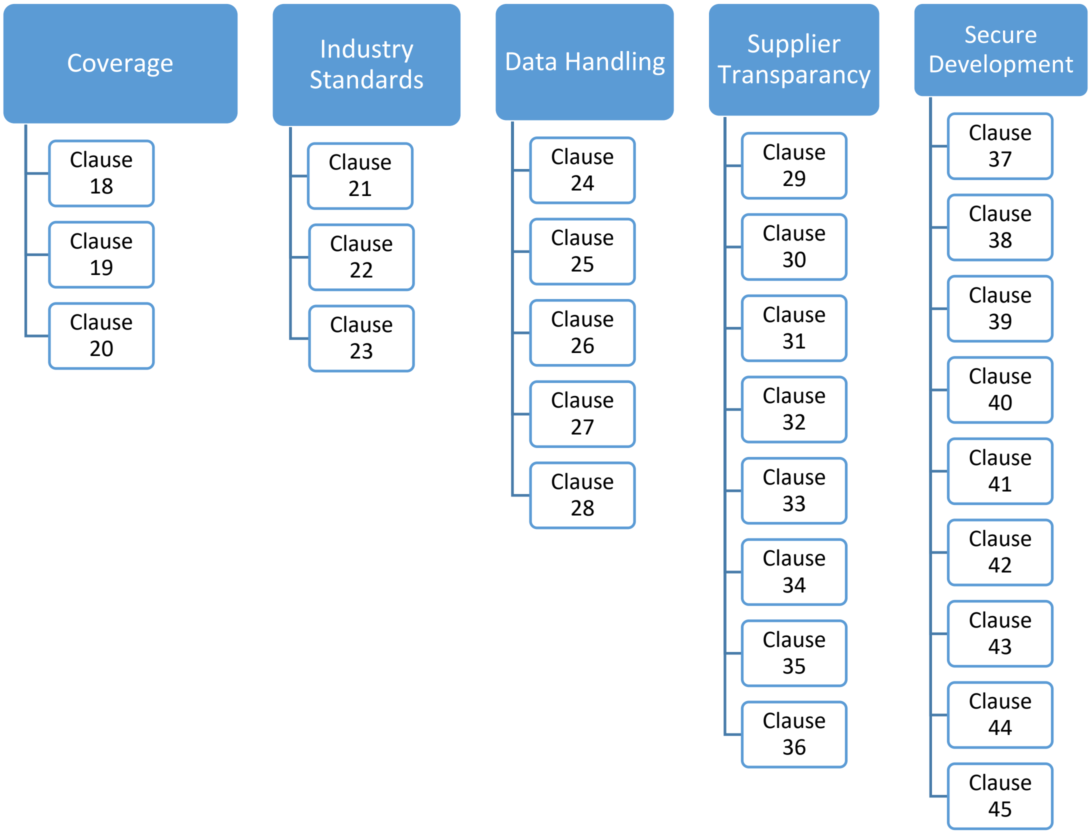
Framework Pillar: Maturity

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
- Current OS Accountability
- Security Patch Program
- Responsible Data Handling

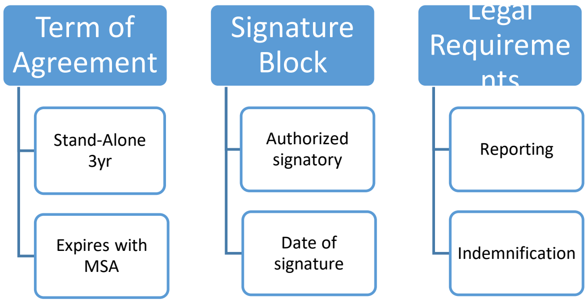
Recommended Clause by Core Principle:



Signature Authority

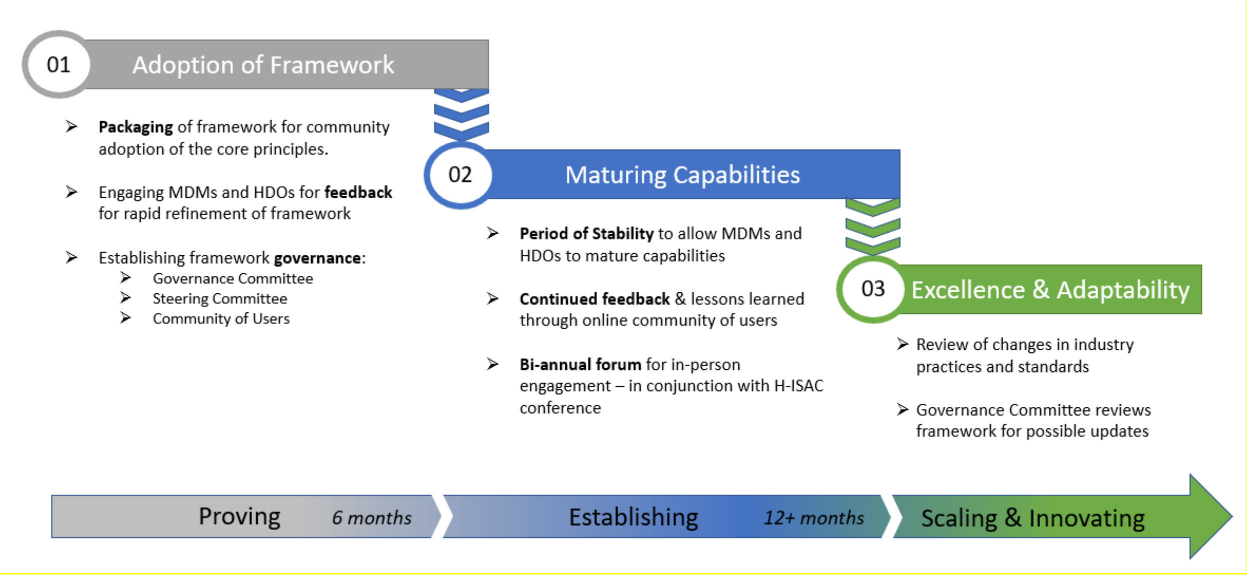
This optional section will indicate the term of the Agreement and the designated signatories required for each party. This section may also include additional legal statements required under the term of the Agreement (Report, Indemnification)

- 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.



01 Adoption of Framework

- **Packaging** of framework for community adoption of the core principles.
- Engaging MDMs and HDOs for **feedback** for rapid refinement of framework
- Establishing framework **governance**:
  - Governance Committee
  - Steering Committee
  - Community of Users

02 Maturing Capabilities

- **Period of Stability** to allow MDMs and HDOs to mature capabilities
- **Continued feedback** & lessons learned through online community of users
- **Bi-annual forum** for in-person engagement – in conjunction with H-ISAC conference

03 Excellence & Adaptability

- Review of changes in industry practices and standards
- Governance Committee reviews framework for possible updates

- 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 # 1: Vulnerability Management

Framework Pillar: **Performance**	Core Principle: **Vulnerability Management**

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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause # 2: Vulnerability Management

Framework Pillar: **Performance**	Core Principle: **Vulnerability Management**

Supplier shall either: a) provide patches and updates that do not modify any Customer-configured preferences and security and privacy settings of Supplier Products, but not including third-party Services, or b) notify the Customer of any patches that do or may possibly modify such preferences and settings.

Supplier shall ensure that Products only accept patches and updates that have been validated as having passed testing by the Supplier or third-party.

Revision History

Proposed Change:	Proposed by:	Date:

<table>
<tr><th colspan="3">Clause ID# 3: Risk Reduction for Care Delivery</th></tr>
<tr><td colspan="2">Framework Pillar: <b>Product Design Maturity</b></td><td>Core Principle: <b>Secure by Default</b></td></tr>
<tr><td colspan="3">For all Supplier designed Medical Devices, 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.</td></tr>
<tr><td colspan="3"><b>Revision History</b></td></tr>
<tr><td>Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="3">Clause ID# 4: Attack Surface Reduction and Hardening</th></tr>
<tr><td colspan="2">Framework Pillar: <b>Product Design Maturity</b></td><td>Core Principle: <b>Secure by Default</b></td></tr>
<tr><td colspan="3">All Supplier Product cybersecurity features shall either be enabled by default or be clearly identified as requiring initial configuration. Product documentation shall specify how to enable, configure, and use all Product cybersecurity features.</td></tr>
<tr><td colspan="3"><b>Revision History</b></td></tr>
<tr><td>Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Clause ID# 5: Secure Development

Framework Pillar: **Product Design Maturity**	Core Principle: **Secure by Default**

Before Supplier-designed Products are delivered to or installed at a Customer location, the Supplier shall verify and document that all software embedded within such Products does not contain any known viruses or malware.

Supplier Products shall install and maintain runtime detection and response capabilities such as:

(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 incidents.

or

(ii) A whitelisting application when the Supplier cannot install an anti-virus / anti-malware application.

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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 6: Access & Credentials

Framework Pillar: **Product Design Maturity**	Core Principle: **Secure by Default**

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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 7: Attack Surface Reduction & Hardening

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security 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

Proposed Change:	Proposed by:	Date:

Clause ID# 8: Secure Development

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**

Supplier shall provide a monitoring system or service designed to detect and prevent abnormal network traffic for hosted services that identifies potential and actual intrusions by unauthorized users. Such monitoring system or service along with other security systems (e.g., firewalls, anti-virus programs or whitelisting) 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. Monitoring system or service logs shall be maintained for a minimum of six (6) years according to HIPAA Guidelines (§164.308(a)(5)(ii)(C); §164.312(b); and §164.308(a)(1)(ii)(D)), or as agreed on by the parties.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 9: Physical Security

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**

Supplier shall design and implement in their Devices 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 Devices in the Customer's environment(s). In some cases, Supplier shall work with the Customer to meet the physical security needs of their Devices.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 10: Physical Security		
Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**	
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		
Proposed Change:	Proposed by:	Date:

Clause ID# 11: Attack Surface Reduction & Hardening		
Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**	
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 whitelisting, or anti-virus / anti-malware software). Supplier represents and warrants that Service removal or disabling will not affect the intended use of the Devices. 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		
Proposed Change:	Proposed by:	Date:

Clause ID# 12: Secure Design

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**

Supplier shall implement Defense-in-Depth security techniques in the development, design, and architecture of Devices to:

(i) During the distribution, deployment, and maintenance of Devices, protect the confidentiality, integrity, and availability of Device Data throughout its lifecycle.
(ii) Throughout any Cybersecurity Event, maintain the critical functionality of Devices.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 13: Data Protection

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**

Supplier shall represent and warrant that Devices shall be able to encrypt at-rest and in-transit Device Data on internal Device storage and on portable media. This functionality shall be in compliance with industry encryption protocols and standards.

When not currently feasible, such as when data cannot be protected with a minimum of TLS 1.2 encryption, 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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 14: Audit Controls

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**

For Supplier-managed Security Controls 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 devices, security devices, authentication controls, and anti-virus/anti-malware for a period of six (6) years according to HIPAA Guidelines (§164.308(a)(5)(ii)(C); §164.312(b); and §164.308(a)(1)(ii)(D)), or as agreed on by the parties.

Supplier shall represent and warrant that Devices can log core operational functions that include but are not limited to:

(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

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 for a period of 6 years according to HIPAA Guidelines (§164.308(a)(5)(ii)(C); §164.312(b); and §164.308(a)(1)(ii)(D)).

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 15: Use of Portable Media

Framework Pillar: **Product Design Maturity**

Core Principle: **Standard Security Controls**

Supplier shall get prior written approval from the Customer in order 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 DVD/CD-ROMs, and on portable devices including but not limited to cell phones, computers, tablets, and endpoint devices.

Supplier shall ensure that when Customer Sensitive Information is stored or maintained on removable or transportable media or on portable devices, 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, including NIST-800-53A.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 16: Secure Development

Framework Pillar: **Product Design Maturity**	Core Principle: **Standard Security Controls**

Supplier shall document and disclose to the Customer authentication procedures for Devices that apply to all hardware, OS, and application authentication. Supplier shall represent and warrant that all authentication methods were designed and implemented against an industry standard such as NIST 800-63B.

Supplier shall disclose to the Customer the design 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, Devices shall require users to change local passwords upon first login.

Where feasible, Devices shall support a central user authentication and authorization system provided by the Customer (e.g., LDAP and Active Directory).

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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 17: Remote Access Method

Framework Pillar: **Product Design Maturity**	Core Principle: **Remote Access Controls**

Supplier shall disclose to the Customer their standard method to remotely access to the Customer's environment that includes but is not limited to:

(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		
Proposed Change:	Proposed by:	Date:

Clause ID# 18: General Compliance

Framework Pillar: **Supplier Maturity**	Core Principle: **Universal Coverage**

Universal Coverage 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 Devices and/or middleware where Data is accessed, collected, stored, and/or transmitted to the Supplier using any method. Universal Coverage shall apply to any form or medium of Data that includes, but is not limited to, visual, electronic, or hard-copy.

Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 19: Service Locations

Framework Pillar: **Supplier Maturity**	Core Principle: **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 in this Agreement. No Service Location may be located outside the United States without the Customer's prior written approval where required by law.

Prior to any change in any Service Location including but not limited to any change in a hosting, data center, and co-location facility or provider, the Supplier will provide written notice and an opportunity for the Customer to review a proposed new facility and/or provider, and/or to conduct a Security Assessment.

Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 20: Supplied Contractors

Framework Pillar: **Supplier Maturity**	Core Principle: **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

Proposed Change:	Proposed by:	Date:

Clause ID# 21: Compliance with FDA Cybersecurity Guidance

Framework Pillar: **Supplier Maturity**	Core Principle: **Industry Standards Alignment**

For all Medical Devices, at a minimum the Supplier

(a) Shall comply with all required and recommended practices set forth in the FDA *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*.

(b) Shall comply with required and recommended practices set forth in the FDA *Postmarket Management of Cybersecurity in Medical Devices*.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 22: Secure Design

Framework Pillar: **Supplier Maturity**	Core Principle: **Industry Standards Alignment**

Supplier shall assess and categorize all potential Device security Vulnerabilities identified in pre- or post-market testing in agreement with the most current published version of the Common Vulnerability Scoring System (CVSS) model. Supplier shall in good faith objectively assess vulnerabilities based on the inherent design of the device and the CVSS model.

Revision History

Clause ID# 24: Offshoring of Customer Controlled Information

Framework Pillar: **Supplier Maturity**	Core Principle: **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

Proposed Change:	Proposed by:	Date:

Clause ID# 23: Vulnerability Management

Framework Pillar: **Supplier Maturity**	Core Principle: **Industry Standards Alignment**

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.

Within two (2) days of the Supplier notifying the Customer of an Uncontrolled Risk, Supplier shall provide the Customer Vulnerability descriptions that conforms with the CVSS model and includes:

a) Risk impact

b) Risk remediation strategy and processes

c) Compensating controls the Customer can implement to mitigate the risk

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 25.0: Data Protection

<table>
<tr><td colspan="2">Framework Pillar: <b>Supplier Maturity</b></td><td>Core Principle: <b>Responsible Data Handling</b></td></tr>
<tr><td colspan="3">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 Device Data that does not reside on the Devices’ end points by implementing industry best security practices at the locations where the Device Data is stored in order to ensure the confidentiality, integrity, and availability of the Device Data and the systems that store the Device Data.</td></tr>
<tr><td colspan="3"><b>Revision History</b></td></tr>
<tr><td>Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="3"><b>Clause ID# 26.0: Data Protection</b></td></tr>
<tr><td colspan="2">Framework Pillar: <b>Supplier Maturity</b></td><td>Core Principle: <b>Responsible Data Handling</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td colspan="3"><b>Revision History</b></td></tr>
<tr><td>Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="3"><b>Clause ID# 27.0: Data Protection</b></td></tr>
<tr><td colspan="2">Framework Pillar: <b>Supplier Maturity</b></td><td>Core Principle: <b>Responsible Data Handling</b></td></tr>
<tr><td colspan="3">Prior to disposal of any Devices returned or discontinued 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.</td></tr>
<tr><td colspan="3"><b>Revision History</b></td></tr>
<tr><td>Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="4"><b>Clause ID# 28.0: Data Protection</b></td></tr>
<tr><td>Framework Pillar: <b>Supplier Maturity</b></td><td colspan="3">Core Principle: <b>Responsible Data Handling</b></td></tr>
<tr><td colspan="4">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.</td></tr>
<tr><td colspan="4"><b>Revision History</b></td></tr>
<tr><td colspan="2">Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="4"><b>Clause ID# 29: Attack Surface Reduction & Hardening</b></td></tr>
<tr><td>Framework Pillar: <b>Supplier Maturity</b></td><td colspan="3">Core Principle: <b>Supplier Transparency</b></td></tr>
<tr><td colspan="4">Supplier shall disclose to the Customer all access account and methods including passwords or authentication methods for those accounts present on Devices at delivery including but not limited to those used for Supplier-provided maintenance and support of devices.
Supplier shall disclose to the Customer all methods for accessing Devices by bypassing any authentication mechanisms for Devices including but not limited to OS-level, application-level, and hardware authentication.</td></tr>
<tr><td colspan="4"><b>Revision History</b></td></tr>
<tr><td colspan="2">Proposed Change:</td><td>Proposed by:</td><td>Date:</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="2"><b>Clause ID# 30: Approved Mitigations</b></td></tr>
<tr><td>Framework Pillar: <b>Supplier Maturity</b></td><td>Core Principle: <b>Supplier Transparency</b></td></tr>
</table>

For all Controls that the Supplier proposes as an alternative to any requirements in this Agreement must be deemed acceptable by the Customer. For alternative Controls deemed by the Customer as unacceptable, the Supplier shall, in good faith, identify industry-standard alternative Controls for Customer review.		
Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 31: Vulnerability Management		
Framework Pillar: **Supplier Maturity**	Core Principle: **Security Patch Program**	
Supplier shall maintain the most up to date third party SW security patches of all Supplier managed infrastructure used to process customer data, deliver services, and solutions, to include all employee devices, network infrastructure, cloud or virtual infrastructure, and any 3rd party hosted infrastructure. Supplier shall apply security patches within 30 days of the patch release and have a formal tracking and plan of action process for any security patches that are not implemented.		
Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 32: Vulnerability Management		
Framework Pillar: **Supplier Maturity**	Core Principle: **Security Patch Program**	
The supplier will design Devices to be capable of accepting all applicable security patches. Installation of these security patches can be applied with or without the support of the Supplier personnel. If unique patching instructions or packaging is needed, the Supplier will provide the necessary information in conjunction with the validation of the patch. If patching can only be completed by the Supplier, the Supplier will commit to the resources needed to patch all applicable devices at all Service Locations.		
Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 33: Vulnerability Management

Framework Pillar: **Supplier Maturity**	Core Principle: **Supplier Transparency**

Supplier shall notify the Customer of all actual or potential security issues associated with any Supplier-designed Product (*Known Vulnerability or Exploit* or KVE), whether identified by the Supplier, Customer, or third-party entity within three (3) business days of KVE identification.

Notification shall include the Supplier's KVE immediate response plan and KVE long-term mitigation plan that include timeframes.

Supplier shall create, implement, and maintain a process to record, track, and report all identified KVEs.

For all suspected and confirmed KVEs, Supplier shall take all actions necessary to assist the Customer and its delegates in investigations of the nature and impact of such KVEs upon the Customer and its facilities, affiliates, and patients. When requested by the Customer, Supplier shall design and implement efforts to mitigate KVE adverse impacts.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 34: Vulnerability Management

Framework Pillar: **Supplier Maturity**	Core Principle: **Supplier Transparency**

Supplier shall coordinate with the Customer to define and document a communications strategy for urgent and non-urgent engagement related to Vulnerability management. The strategy must at a minimum outline the key strategic contacts for both the Supplier and Customer, logistics for engagement, and applicable Service Level Agreements (SLAs) for engagement.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 35: Incident Management

Framework Pillar: **Supplier Maturity**	Core Principle: **Supplier Transparency**	
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.		
Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 36: Vulnerability Management

Framework Pillar: **Supplier Maturity**	Core Principle: **Supplier Transparency**	
Supplier shall disclose to the Customer all known impacts to the safety of individuals or potential data exposure based on any Device Vulnerability being exploited. Supplier shall document and disclose to the Customer all changes in Device safety, functionality, performance, and/or user instructions that result from Device Vulnerability remediation in adherence to ISO 14971.		
Revision History		
Proposed Change:	Proposed by:	Date:

Clause ID# 37: Secure Design

Framework Pillar: **Supplier Maturity**	Core Principle: **Security Development Lifecycle**
Supplier shall represent and warrant that it performed Security Assessments of potential Device security vulnerabilities, threats, and risks as part of Device 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) *Frameworks for Improving Critical Infrastructure Cybersecurity* and the	

Open Web Application Security Project (OWASP) *Internet of Things Framework Assessment*. Supplier shall disclose the standards used for assessment.

Supplier shall score the Vulnerabilities according to the Common Vulnerability Scoring System (CVSS) model.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 38: Secure Code Design & Analysis

Framework Pillar: **Supplier Maturity**	Core Principle: **Security Development Lifecycle**

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 and tools shall include static code analysis tools designed to discover security vulnerabilities in Code.

Supplier represents and warrants that it shall resolve any findings (for example, warnings or violations) produced by such tools prior to the delivery of Code to the Customer, or if not resolved, provide evidence that the findings shall not affect the security of Products under their intended use.

Supplier shall ensure that all third-party Device software is developed using secure coding practices as part of a software development lifecycle that includes assessing all Device software to eliminate vulnerabilities described in the OWASP Top 10 and the CWE/SANS Top 25 most dangerous software errors. Supplier shall develop and maintain a quality assurance program for Device software that identifies and corrects potential vulnerabilities.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 39: Privileged Access

Framework Pillar: **Supplier Maturity**	Core Principle: **Security Development Lifecycle**

Supplier shall design and/or configure each Device component to operate using the principle of least privilege (PoLP), including but not limited to operating system permissions, file access, user accounts, and application-to-application communications.

Supplier represents and warrants that Devices isolate Code, processes, and data, from Device 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-designed Products shall not require any dependencies for application, commercial software, service, or communication processes to have System or Device administrative privileges to function.

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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 40: Operating System

Framework Pillar: **Supplier Maturity**	Core Principle: **OS Accountability**

Supplier shall identify the Operating System (OS) and all software in its Devices. Devices 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 device is running an OS within two (2) years of obsolescence, the Supplier shall upgrade the Device to a non-obsolete OS, at the Supplier’s expense.

For all Devices 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 Devices 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.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 41: Penetration Testing

Framework Pillar: **Supplier Maturity**

Core Principle: **Security Development Lifecycle**

Supplier shall implement pre- and post-market Software Development Life Cycle (SDLC) Penetration testing of all Products. If testing identifies Vulnerabilities that have an industry-standard critical, high, or uncontrolled nature, Supplier shall develop a remediation action plan within thirty (30) days that follows industry best practices such as ISO 29147, ISO 30111, the FDA *Postmarket Cybersecurity Guidelines*, and the FDA *Postmarket Management of Cybersecurity in Medical Devices*.

For all identified Vulnerabilities, Supplier shall notify the Customer within thirty (30) calendar days and shall mitigate or remediate within sixty (60) calendar days.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 42: Penetration Testing (hosted & cloud solutions)

Framework Pillar: **Supplier Maturity**

Core Principle: **Security Development Lifecycle**

In cooperation with Supplier, the Customer or an experienced third-party of the Supplier's choosing can 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 application security Vulnerability scanning, application penetration testing, static analysis, and/or manual code review.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 43: Penetration Testing

Framework Pillar: **Supplier Maturity**	Core Principle: **Security Development Lifecycle**

Customer shall conduct Security Assessments prior to engaging Supplier to perform Secure Services and on an annual basis thereafter (unless a different frequency is specified in the applicable agreement between the parties). In the event of a security breach that involves Customer Sensitive Information attributable to Supplier's performance of Secure Services, Customer may require more frequent Security Assessments and/or additional actions or Controls, including but not limited to those set forth in the applicable agreement between the parties.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 44: Vulnerability Management

Framework Pillar: **Supplier Maturity**	Core Principle: **Security Development Lifecycle**

Supplier shall provide a complete Software Bill of Material (SBOM). For the supported life of the medical device, the supplier shall monitor for security vulnerabilities in these software components and use a risk-based approach to mitigate any severe and exploitable vulnerabilities.

An SBOM shall contain the minimum elements as and when defined by the FDA or other industry guidance, standard, or regulation

In the event the software component ceases to be actively maintained, the Supplier shall notify the Customer and either replace the software component with an actively maintained equivalent or assume active maintenance internally of the software component.

In the event the maintainer of a software component changes to a new maintainer, the Supplier shall notify the Customer and perform through cybersecurity testing of any subsequent releases of the software component, before placing the new versions into active use.

Revision History

Proposed Change:	Proposed by:	Date:

Clause ID# 45: Vulnerability Management

Framework Pillar: **Supplier Maturity**

Core Principle: **Supplier Transparency**

Supplier shall disclose to the Customer all known impacts to the safety of individuals based on any Device Vulnerability being exploited.

Supplier shall document and disclose to the Customer all changes in Device safety, functionality, performance, and/or user instructions that result from Device Vulnerability remediation in adherence to ISO 14971.

Revision History

Proposed Change:	Proposed by:	Date:

Contract Clause Definitions:

The definitions provided below are generally harmonized with the NIST CSRC Glossary: https://csrc.nist.gov/glossary/term/security_service

Agreement
This contract document.

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 Devices.

Controlled Risk
As defined by FDA 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

	Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device’s particular cybersecurity vulnerability.
Customer	Medical corporation and its business lines, employees, and patients that uses Products provided by the Supplier.
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.
Fail Safe	Fail-Safe' refers to the ability of a Device 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.

MDS2	Manufacturer Disclosure Statement for Medical Device Security
Medical Device	As defined by the FDA https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device.
Non-medical Device	Device that is not a Medical Device.
Product	Device, Service, or Solution provided by the Supplier to the Customer.
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 Devices.
Security Control	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 (https://niccs.us-cert.gov/about-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 (https://niccs.us-cert.gov/about-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 Device 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 Devices to the Customer.

Uncontrolled Risk

"As defined by FDA 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

Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations.

Universal Coverage

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

Vulnerability	Actual or potential cybersecurity threat or risk to a device or system

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 to must contract language. The HSCC intends to review and update this reference as experience and recommended improvements dictate. 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 device design and management. Please send your comments at any time to: ContractsFeedback@HealthSectorCouncil.org.

Acknowledgments

The Health Sector Coordinating Council 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 this resource.

In particular, we wish to thank:

Michelle Bentley, Mayo Clinic (Chair)

Jason Ferri, Premier (Chair)

Jim Jacobson, Siemens Healthineers (Chair)

Jonathan Bagnall, Royal Philips

Erik Berg, Siemens Healthineers

Jake Bronowski, Froedtert

Angelo Calvache, Accuray

Justin Cooper, Sentara Healthcare

Terri Duket, GE Healthcare

Stephen Dunkle, Geisinger

Christopher Falkner, Sodexo North America

Thom Floyd, Royal Philips

Chris Gates, Velentium

Ed Gaudet, Censinet

Ty Greenhalgh, Cyber Tygr, LLC

Linda Hillen, Abbott

Shawna Hofer, St. Luke's Health

Emily Holmquist, Medtronic

Terry Hutton, Sentara Healthcare

Mike Kushner, Kaiser Permanente

Matt McMahon, Royal Philips

Curt Miller, Healthcare Supply Chain Association

Kyle Neuman, DirectTrust

Mike Powers, Intermountain Health

Marc Sammons, Health Trust

Andrew Sargent, Instrumentation Laboratory

Eirene Shipkowitz-Smith, Baxter Healthcare

Kevin Tambascio, Cleveland Clinic

Shayana Vasichek, Abbott

Varun Verma, Royal Philips

Alex Wolf, Cleveland Clinic

Oleg Yusim, Edwards Lifesciences