Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

MEDICAL DEVICE AND HEALTH IT JOINT SECURITY PLAN

January 2019

ABOUT THE HEALTHCARE AND PUBLIC HEALTH SECTOR COORDINATING COUNCIL CYBERSECURITY WORKING GROUP

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 and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

This Medical Device and Health IT Joint Security Plan is the product of a task group established under the auspices of the HSCC CWG and composed of medical technology, health IT and health delivery organizations, as well as the FDA, to address a major recommendation of the Health Care Industry Cybersecurity Task Force report from June 2017 calling for a cross-sector strategy to strengthen cybersecurity in medical devices.

To provide feedback on this tool, please send comments to:
JSPFeedback@HealthSectorCouncil.org

For more information on the HSCC, see https://HealthSectorCouncil.org.

`

Contents

I Acknowledgments

The following individuals constitute the membership of the committee established in November 2017 who were responsible for development of the Medical Device and Healthcare Information Technology Joint Security Plan.

- **Task Group Co-Chair,** Kevin McDonald, Director of Clinical Information Security, Mayo Clinic
- **Task Group Co-Chair,** Rob Suarez, Director of Product Security, Becton, Dickinson & Company
- **Task Group Co-Chair,** Aftin Ross, Senior Project Manager, Center for Devices and Radiological Health (CDRH) at US Food and Drug Administration
- Bill Hagestad, Independent Information Security Researcher
- Colin Morgan, Director, R&D & Product Security, Johnson & Johnson
- Jim Jacobson, Chief Product and Solution Security Officer, Siemens Healthineers
- Michael McNeil, Global Product Security & Services Officer, Philips
- Seth Carmody, Cybersecurity Project Manager, CDRH at US Food and Drug Administration
- Zach Rothstein, Vice President, Technology and Regulatory Affairs, AdvaMed
- Ronald Mehring, Chief Information and Security Officer/VP of Technology, Texas Health Resources
- Hitesh Patadia, Enterprise Architect, Alberta Health Services
- Christopher Bennett, Senior Information Security Analyst, Medical University of South Carolina
- Greg Garcia, Executive Director at Healthcare Sector Coordinating Council
- Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, CDRH at US Food and Drug Administration
- Caleb Eggink, Security Solution Leader, Cerner
- Ali Nakoulima, Lead Technology Architect, Cerner
- Regina Geierhofer, Regulatory Affairs Manager, Cerner
- John Travis, Vice President Regulatory Research, Cerner

`

- Ray Smith, Lead Software Engineer, Cerner
- Greg Thole, Senior Regulatory Strategist, Cerner
- Wil Vargas, Standards Director, Association for the Advancement of Medical Instrumentation
- Jim Hanson, Information Security Officer, Avera Health
- Ashley Woyak, Business Information Security Officer, Baxter Healthcare Corporation
- Ken Hoyme, Director of Product Security, Boston Scientific
- Michael Maksymow, CIO, Beebe Healthcare
- Michael Seeberger, Systems Engineer, Boston Scientific
- Mari Rose Savickis, Vice President of Federal Affairs, CHIME
- Fernando Blanco, CHRISTUS Health, VP & CISO
- Aaron Wishon, CISO, Cook Children's Health Care System
- Clyde Hewitt, Vice President, Security Strategy / NCHICA Board of Directors, CynergisTek/NCHICA
- David Klonoff, President, Diabetes Technology Society
- Charles Stride, Senior VP, CIO/CISO, Holy Redeemer Health System,
- Paul Connelly, VP/CISO, HCA Healthcare
- Peter Amadio, Professor of Biomedical Engineering, Mayo Clinic (AEHIS)
- Greg Garneau, CISO, Marshfield Clinic Health System
- Lisa Griffin Vincent, VP of Clinical Science, Medical Device Innovation Consortium
- Elliott Warren, Director of Federal Affairs, Medical Device Manufacturers Association
- Zack Hornberger, Director of Cybersecurity & Informatics, Medical Imaging Technology Association
- Matt Russo, Sr. Director of Global Security Office, Medtronic
- Ari Entin, CIO, Natividad Medical Center (AEHIS)
- Katie Boyer, Manager of Policy and Advocacy, Nemours Children's Health System

`

- Jon Crosson, Manager of Special Interest Group Services, H-ISAC
- Nathan Gibson, CIO, Quality Insights (AEHIS)
- Dr. Sheila Whalen, DNP, RN-BC, Clinical Integration Program Manager, Rush University Medical Center
- Kevin Scott, Senior Corporate Director of Security and End User Services, Shriners Hospitals for Children
- Ross Carevic, Director of Business Technology, Vizient
- Christine Sublett, President &Principal Consultant, Sublett Consulting, LLC
- Alex Reniers, Cyber Analyst, US Department of Homeland Security

The HSCC Cybersecurity Working Group TG-1B drafting committee would also like to thank all of the individuals and organizations within the Healthcare Sector Coordinating Council (HSCC) that reviewed and contributed to the plan.

`

II Executive Summary

Software-based medical technologies have the potential to positively impact patient care. However, as these products become more connected, product cybersecurity becomes increasingly important as there is the potential for patient harm and disruption of care if products or clinical operations become impacted because of a cybersecurity concern. As product cybersecurity is a shared responsibility, a wide range of healthcare stakeholders under the umbrella of the Healthcare and Public Health Sector Coordinating Council (HSCC), have drafted this Joint Security Plan (JSP) to address cybersecurity challenges. These challenges include but are not limited to transparency and disclosure between vendors and end users, security by design and throughout the product lifecycle, and product end of life. Specifically, the JSP is a total product lifecycle reference guide to developing, deploying and supporting cyber secure technology solutions in the healthcare environment. It includes:

- Cybersecurity practices in design and development of medical technology products
- Handling product complaints relating to cybersecurity incidents and vulnerabilities
- Managing security risk throughout the lifecycle of medical technology
- Assessing the maturity of a product cybersecurity program

The JSP is voluntary and seeks to aid organizations (medical device manufacturers, healthcare information technology (IT) vendors, and healthcare providers) in enhancing their product cybersecurity irrespective of organization size or maturity. It is intended to be globally applicable, inspire organizations to raise the bar for product cybersecurity, and is expected to evolve as product cybersecurity evolves. As such, it is anticipated that there will be future iterations of the JSP and feedback on this initial version is welcome.

It is important for medical device manufacturers (MDMs) and health IT vendors, collectively referred to as vendors, to consider the JSP's voluntary framework and its associated plans and templates throughout the lifecycle of medical devices and health IT because doing so is expected to result in better security and thus better products for patients. Security can be difficult to integrate into existing processes for a variety of reasons such as organizations not recognizing its importance, not knowing where to start, and insufficient resources. The components in the JSP framework are used to help create security policy and procedures that align and integrate into existing processes. Our primary ask of organizations is to make a commitment to implementing the JSP as it is expected that patient safety will be positively impacted as a result.

III Background

In the *Cybersecurity Act of 2015* (the Act), the United States Congress established the Health Care Industry Cybersecurity (HCIC) Task Force to identify the challenges that the healthcare industry faces when securing and protecting itself against cybersecurity threats. Industry participation in the task force brought to light critical gap areas warranting focus; year-long discussion and analysis culminated in the release of a set of recommendations and action items to address six high-level imperatives.

In 2017, a group of medical device manufacturers stepped up to address the recommendations and action items set forth under Imperative 2 of the HCIC Task Force Report: "Increase the security and resilience of medical devices and health IT" by engaging healthcare delivery organizations in a collaborative effort that would produce a Joint Security Plan. This effort was further formalized under the auspices of the Healthcare Sector Coordinating Council's Joint Cybersecurity Working Group public-private partnership, as the JSP was broadly socialized with healthcare providers, trade associations, security professionals, and government organizations during development and prior to its release. The U.S. Food and Drug Administration, in its role as a key public sector partner, also assisted with the development of the JSP. For additional information on how the JSP was drafted, please see Appendix D. Imperative 2 of the HCIC Task Force Report states:

> ***Imperative 2. Increase the security and resilience of medical devices and health IT.***
>
> *The Health Care and Public Health (HPH) Sector is charged with keeping patients safe and that includes protecting patients from physical harm, as well as privacy-related harms that may stem from an exploited known cybersecurity vulnerability. If exploited, a vulnerability may result in medical device malfunction, disruption of health care services (including treatment interventions), inappropriate access to patient information, or compromised EHR data integrity. Such outcomes could have a profound impact on patient care and safety. Some foundational challenges that will need to be addressed in order to enhance the cybersecurity of medical devices and EHRs include legacy operating systems, secure development lifecycle, strong authentication, strategic and architectural approaches to product deployment, management, and maintenance on hospital networks.*
>
> *The relatively short lifespan for operating systems and other relevant platforms such as commercial off the shelf software is inherently misaligned in health care as medical devices and EHRs may be utilized for 10, 15, 20, or more years. This misalignment may occur for a variety of reasons. Hospitals operate on thin budgets and cannot replace capital equipment like MRIs as quickly as new operating systems are released. Product vendors have a product development lifecycle that may take several years and they may start development using one operating system and by the time the product comes to market, newer operating systems may be available. Creative ways of addressing the aforementioned challenge areas may be found by engaging key clinical and cybersecurity stakeholders, including software vendors.*

The JSP is expected to evolve over time and the HSCC intends to establish a governance model to ensure the baseline strategy is updated based on execution of existing plans or new needs identified by members of the stakeholder community.

IV Purpose and Objectives

The HSCC believes that, because medical technology is integral to patient safety and clinical operations, product cybersecurity in medical technology is a shared responsibility among healthcare stakeholders. Moreover, more secure products result in higher quality products which positively impact public health. The JSP is a consensus-based total product lifecycle reference guide for developing, deploying, and supporting cyber secure technology solutions in

the health care environment. It is not a regulatory document nor is it a standard. Rather the JSP may be leveraged across an organization's product portfolio and is intended to be globally applicable. Furthermore, the recommendations provided in the JSP are intended to help organizations of various size and stages of maturity to enhance their product cybersecurity posture by addressing key cybersecurity challenges.

This voluntary plan is intentionally forward leaning and seeks to inspire organizations to raise the bar for product cybersecurity. In particular, integrating cybersecurity into an organization necessitates organizational and process changes that come with considerable time and monetary investments. The JSP provides a framework for making these organizational and process related changes.

One of the main themes of the JSP is the idea of continuous improvement. We encourage medical device manufacturers, health IT vendors, and healthcare providers to make a commitment to adopting the JSP to aid in developing, deploying, and supporting cyber secure technology solutions in the health care environment. The adoption of the JSP, with the integration into current practices, is expected to provide a safer and more resilient patient care and result in overall improved product quality.

V JSP Product Security Framework Overview

The JSP framework establishes that effective cybersecurity is integrated into an organization's quality system processes and is incorporated throughout the various stages of the commercialization process (from concept to launch). Figure 1 provides a framework for incorporating the JSP into existing quality system processes and throughout commercialization. The core of this framework aligns to traditional quality system concepts. Design controls, risk management, design requirements, testing and post market management can be aligned with multiple software development methodologies (not shown). Documentation of the product security activities/processes in the JSP framework core is encouraged to demonstrate that the framework has been applied consistently and is rigorously followed. Healthcare providers seeking further guidance on the secure operation of medical devices, and other information technology used to run their healthcare operations, may refer to HSCC "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients" publication, which stems from the Cybersecurity Information Sharing Act of 2014 (CISA) 405(d) effort. Additional guidance and detail are provided for each product security activity or process identified in the JSP framework in Section VII of this document. Acronyms and term definitions used throughout the JSP may also be found in Appendix A and Appendix B respectively.

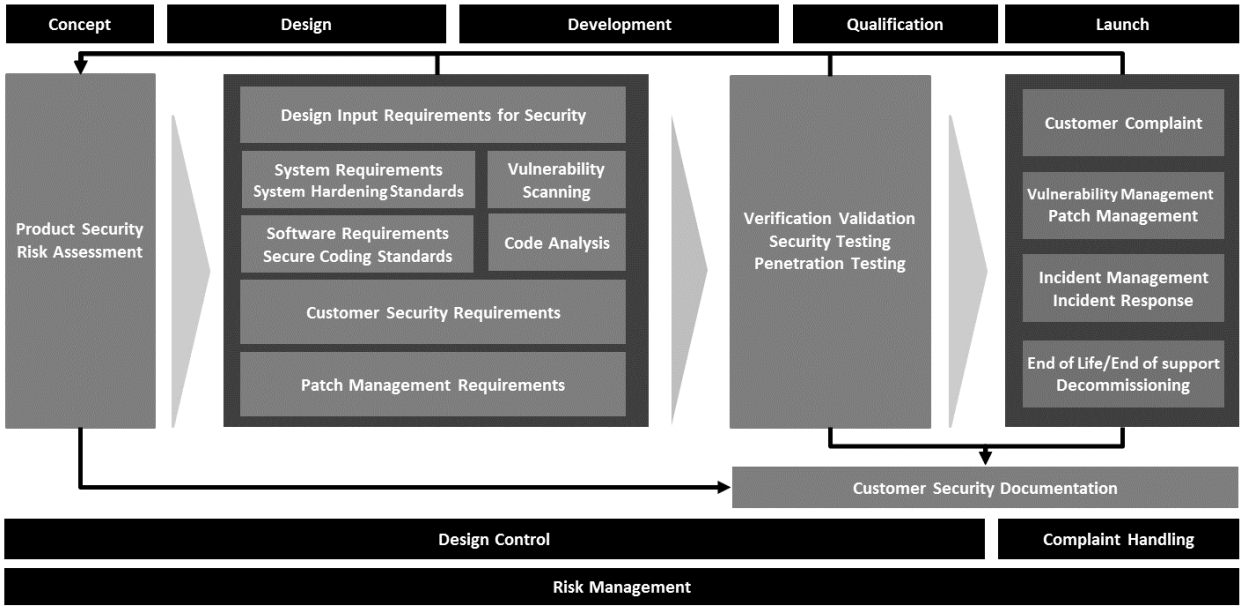

Figure 1. Product Security Framework. Top row represents product commercialization phases. Core represents product security activities and processes. Two bottom rows represent quality system processes

VI How to Use the JSP

For the successful use of the JSP, an initial step is to be able to define the governance process as it relates to organizational roles and responsibilities, and the needs for personnel training.

Governance which may include strategic decisions, establishing milestones, and tracking of maturity against the framework is executed by designated leaders in a vendor's organization. Framework adoption should be driven by mapping each of the framework cybersecurity activities and processes into existing processes and minimizing the creation of separate or redundant processes. Again, the goal of implementing the JSP is to generate higher quality products that positively impact patient safety.

In addition to organizational leadership, various members of the organization have a shared responsibility for product security and thus benefit from the implementation of the JSP. For example, a vendor may share its evaluation of maturity against the JSP with customers. The vendor may also share this information with the HSCC with the intent of informing future iterations of the JSP. Additional granularity regarding stakeholder roles and responsibilities as well as potential organizational structures for implementing security are found in Appendix C and Appendix H respectively.

Organizations adopting this framework should consider providing existing personnel with necessary training to achieve focused incorporation of cybersecurity expertise (see Appendix I

for additional granularity regarding on organizational training). Maintaining functional competency can best be achieved by establishing a routine training regimen or periodic re-assessment of need.

VII JSP Product Security Framework Implementation

This section expands and articulates on security activities and processes in the JSP framework (see Figure 1) in the context of where they align with traditional quality systems processes, and cross references appendices with applicable examples and templates. The goal in adopting the JSP is to integrate the security activities and processes in the JSP framework into existing processes where applicable. For additional information regarding the authoritative sources that were used to draft the content that follows, please see Appendix D.

A. Risk Management

Product security risk assessment is an integral component of overall product risk management. There are specific considerations necessary for ensuring cybersecurity risks identified during design, development, or post launch complaint handling are properly analyzed, evaluated, and documented. This section describes risk management from product concept through product launch.

i. Risk Register

A risk register, also referred to as a risk log, may be standalone or multiple repositories, which can be used to report on efforts across the framework activities, track remediation, and map new known vulnerabilities or potential risks. For vendors, the risk register will be populated from product portfolio management and information from the cybersecurity management plans as described below. Customers also benefit from maintaining a risk register based on information from customer security documentation (see Section VII, Design Control, subsection vi(b) for a description of customer security documentation) and vulnerability disclosures from vendors.

ii. Cybersecurity Management Plan

Beginning at the concept phase, a plan is created to establish how cybersecurity will be managed throughout the product lifecycle of the vendor's product. This plan is maintained throughout the product lifecycle and includes:

- Reports for product security risk assessment, penetration testing, static code analysis, and vulnerability scanning
- Documentation of secure coding standards and system hardening standards applied during development and at installation
- Plans for incident management, vulnerability management, and patch management
- Documentation of service, remote support, and decommissioning procedures which may also be reflected in service contracts
- Customer security documentation that is ready for customer distribution
- Documentation of exceptions (see Section VII, Compliant Handling and Reporting, subsection v for a description of exceptions)

`

This management plan should be cross-functionally reviewed and approved by business leadership in a vendor's organization. Components of this plan necessary for operation and management of product security are provided to customers by inclusion in customer security documentation, user manuals, and reflected in contractual agreements between the vendor and customer.

iii. Product Security Risk Assessment

Product Inventory

Document and maintain a comprehensive list of all software enabled products, product versions, solutions, and services commercially available, in support or in development, in order to track cybersecurity risks.

Security risk assessment may be performed as part of or separately from other types of risk assessment, including those described in ISO 14971. The objective of risk assessment for known vulnerabilities or potential cybersecurity risks is to determine the comprehensive impact, for example, to clinical safety, business operations, intellectual property, patient privacy, contractual requirements, regulation, and law. The risk assessment will also enable the risks and vulnerabilities to be prioritized for response. Figure 2 is an example of: the sources from which a known vulnerability may be identified; the analysis categories used to score the vulnerability; and the output of the risk assessment. Risk assessments should reflect the target operational environment and use case of the product.

Known common vulnerabilities and exposures (CVEs) identified in design and development or during complaint investigation of a launched product are analyzed and evaluated using a consistent vulnerability scoring methodology. One methodology that may be leveraged is the common vulnerability scoring system (CVSS). If CVSS is used, the latest version available should be used at the time of risk assessment to derive the level of cybersecurity risk and information that may be further used in preliminary hazard analysis (PHA), failure mode and effects analysis (FMEA), or other risk assessment tools not specific to cybersecurity, as indicated in Figure 3. Utilizing the most recent version of CVSS can help in this analysis and avoid challenges with determining exploitability for security risks. For many vulnerabilities, CVSS scoring may already be provided based on original equipment manufacturer (OEM) or industry evaluation, but it is recommended that CVSS is calculated specific to the product's implementation with consideration for worst case scenarios where implementation is not strictly controlled (See Appendix J for more information on a draft CVSS rubric for the healthcare context which may aid in this assessment).

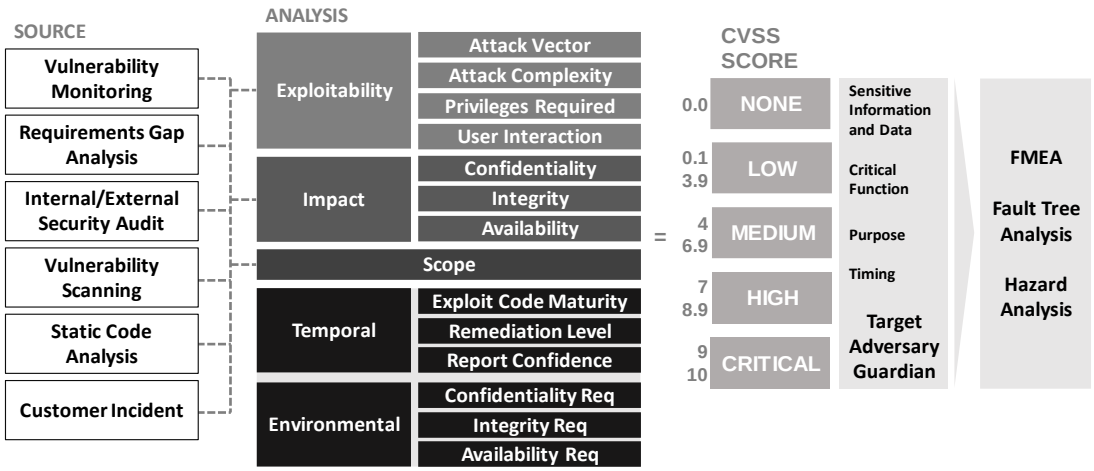

Figure 2. Risk Assessment Sources. Assessing risk from different sources and generating severity scoring that may be used in safety-related risk assessment.

As it relates to Figure 2 above:

- None to low risk means negligible or no impact to confidentiality, integrity, or availability of the patient, user, vendor or customer environment (environmental) which may be considered controlled risk.
- Medium to high risk means potential known vulnerabilities that may result in adverse events impacting confidentiality, integrity, or availability to the patient, user, vendor or customer environment which otherwise may be considered uncontrolled risk depending on impact to safety and efficacy.
- Critical risk introduces potential for injury or harm to patients or users of products including impact to sensitive information and data or critical functions which otherwise may be considered uncontrolled risk.

`

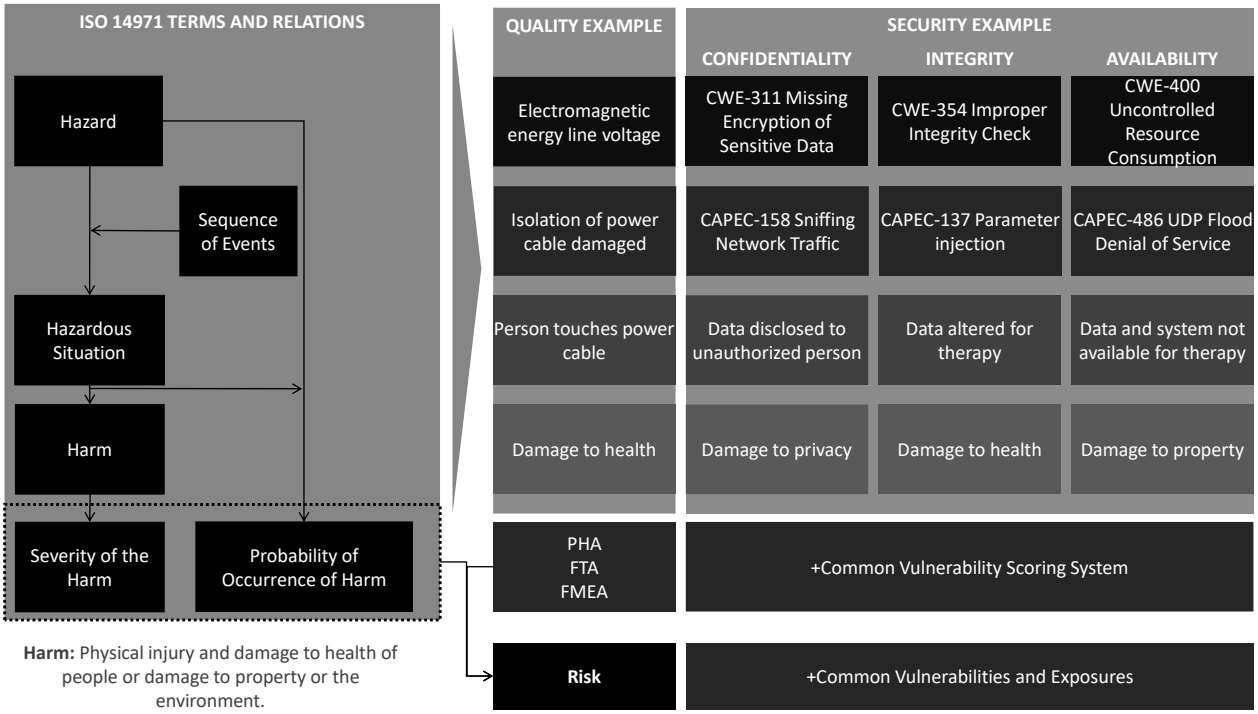

Figure 3. Risk Assessment Mapping. Illustration of how a safety-related risk management process maps to a security-related issue for medical technology

iv. Additional Risk Management Areas

Supply Chain

Secure, according to a vendor information security policy, development and manufacturing environments such that additional security risk is addressed prior to deployment of a product to a customer. These measures should include malware protection measures, file system integrity checking, and access control for intellectual property during the supply chain process.

Third-Party Entities

It is important that external entities involved in the product lifecycle of a medical device or healthcare information technology ensure applicable components described in the JSP framework (Figure 1) can be achieved. Furthermore, by undergoing routine assessment against the applicable components of this framework, third-party entities demonstrate their commitment to further bolstering the state of medical device and health IT security. Additional granularity is provided in an example of a third-party security agreement in Appendix F.

B. Design Control

Design controls consist of policies and procedures that ensure that product design inputs are met so that correct requirements can be developed. For cybersecurity, organizations apply applicable standards and testing to software code during product development as well as during each software release. These design control principles also apply to components provided by third-parties that are used in finished products. The section that follows describes components of the

JSP security framework relevant to design control from product concept through product qualification.

i. Design Input Requirements for Security

As a subset of design input requirements, establish high-level security requirements based on: authoritative sources for security standards and best practices; a vendor's own security requirements when they verifiably exceed existing standards; regulatory requirements for security of technology or medical technology specifically, and customer feedback relating to security. These requirements should be assessed for applicability to a product during the design and development processes (Figure 1). Additional specifics regarding some of these requirements are found in Appendix E. It is expected that additional information regarding cybersecurity vulnerabilities may be obtained once the product is launched. As a result, it is important to incorporate known cybersecurity vulnerabilities and relevant compensating controls into the design control process (i.e. into design control policy and procedures).

ii. System Requirements, System Hardening Standards, and Vulnerability Scanning

- Identify, apply and maintain system hardening standards provided by a third-party component vendor or an authoritative source for securely configuring all products and components used in a vendor product. See Appendix D for examples of authoritative sources for standards and testing.
- Perform vulnerability scanning periodically throughout product development and conduct automated testing to ensure secure system configuration and patching.

iii. Software Requirements, Secure Coding Standards, and Code Analysis

- Apply secure coding standards during the development of software that outline secure coding practices generic to any programming language, and language-specific secure coding standards specific to a programming language.
- Perform static and dynamic code analysis periodically throughout product development testing and integrate automated solutions into development tools to ensure secure coding standards are followed.

iv. Patch Management Requirements

Routinely identify, apply and maintain system-patching throughout the product development process for products and components, including those provided by third-parties. Consider remediation planning within a reasonable timeframe - including an upgrade of the products and components - if patches are no longer supported by their third-party vendor. The deployment and application of patches will have a defined time of disruption to system operation and minimal impact on availability for patient care. See Section VII, Complaint Handling and Reporting, subsection vi for additional granularity on vulnerability and patch management once the product is launched.

v. Security Testing

- Conduct robustness testing during unit and integration testing of proprietary software in development; test interfaces such as user interfaces, network protocols, and file inputs for ability to withstand and handle potentially malicious

input, as well as denial of service attacks and events; and apply standard IT practices such as vulnerability scanning.

- Conduct penetration testing. It is paramount that an independent entity trained and/or certified in cybersecurity verifies cybersecurity testing performed and security controls implemented during design control, as well as in each software release near or at completion of risk remediation. Additionally, they may apply custom cybersecurity testing methodologies based on threat modeling to ensure comprehensive use case coverage. Based on product complexity, connectivity, and integration with customer environments and reliance on customer security controls, a penetration test is recommended on the product in its deployed configuration prior to customer use. Documentation by the vendor of penetration testing reports is critical to include in product design documentation and the cybersecurity management plan; include unmitigated findings in customer security documentation.

vi. Customer Security Requirements

a) Service and Support Access

When remotely or locally accessing customer systems, it is critical that a vendor maintain permissible security and privacy controls and adhere to customer information security policies. Support tools and processes should be monitored for vulnerabilities and insecure practices. The vendor is responsible for providing customer security documentation which comprehensively describes the control measures implemented. In particular, vendor service and support personnel in collaboration with customers are responsible for:

- Obtaining consent from the customer prior to accessing customer environments in addition to uniquely identifying service and support personnel upon authentication and authorization to a system. Also, document processes for how and when local and remote access is performed for service and support.
- Avoiding inclusion of any credentials in product information documentation such as service manuals, which may allow unauthorized access to the product. Default passwords or credentials may be documented when instructions are provided to make those credentials unique.
- Ensuring system cybersecurity controls are always returned to intended configuration prior to completing any vendor service and support visit.

In addition:

- Credentials and passwords should be unique, changed on a regular basis and immediately removed or changed following any service personnel termination.
- Remote access should be done using some type of multi-factor authentication.
- Customer data, including patient data, may never leave the site without written consent and approval from the customer. Data should be de-identified when possible and a clear communication of use of the data must be provided.
- Any use of removable media should be approved by customers and customer information security policies should be adhered to before utilization.

`

- Decommissioning or transfer of products and components from a customer facility, or removal for refurbishment, requires any sensitive information and data to be destroyed or transferred with reasonable and appropriate safeguards with the customer's written authorization.
  - Customers may accept responsibility to destroy sensitive information and data from any product if they wish to do so. Clearly document and follow any federal and local regulatory or legal procedures for transfers of this data.
  - Service may determine approved methods for managing sensitive information and data. In accordance with customer data retention requirements, the destruction of this data must be clearly documented and follow any local regulatory or legal procedures.

b) Customer Security Documentation

For any commercialized product, it is critical that the vendor develop and maintain documentation which describes all pertinent security information related to the product. Furthermore, customer security documentation needs to be updated when significant changes occur in existing or new product versions. This documentation is prepared for external distribution and consumption by customers. Customers, in turn, are responsible for processing vendor-provided customer security documentation to complete questionnaires, agreements, and/or risk assessments during product procurement phases and incorporating results into a risk management platform as well as an asset management platform for ongoing management.

Customer security documentation provided by vendors includes:

- All components provided or required for use, also known as a bill of materials, using the common platform enumeration convention and major version number. This would include components such as software (commercial and open source) and firmware required for device operation
- Description of secure configuration
- Data flow diagrams that capture items flowing in and out of the device, open network ports and active services, as well as any requirements for network connectivity
- Remote access methods and tools, if used
- Access control design including privileged access controls and vendor maintenance and/or service accounts
- Comprehensive description of the control measures implemented
- Patch management plan developed by the vendor that identifies any customer responsibility as part of the plan
- Required cybersecurity controls including malware protection that supported the vendor risk assessment
- Logging and audit capabilities to support customer security operations

- Assumptions and requirements at installation and in use to maintain security
- Summary of known security risks and considerations, including unmitigated findings from penetration testing
- Contact information for the vendor to report incidents, vulnerabilities, or for general inquiries regarding security

For context regarding what may be included in customer security documentation and what it might look like, see Appendix G.

C. Complaint Handling and Reporting

Gathering feedback on the cybersecurity performance of their products post product launch is important for vendors, and complaints are a mechanism for obtaining this feedback. The section that follows provides insight into the types of information vendors may receive and actions they may take as a result.

i. Customer Complaint Escalation

Customer complaint evaluation or investigation by the vendor includes steps to determine if there is a product-related cybersecurity vulnerability or incident. A cross-functional team may be assembled to ensure a coordinated investigation and appropriate response. Specifically, the investigation includes close coordination with the affected customers and appropriate parties. Ensure effective escalation and triage by having adequate procedures and classification for potential cybersecurity issues for handling by service and support. Customers and vendors should perform timely information sharing during an investigation to support rapid response.

If the customer product complaint is associated with protected health information or personally identifiable information, then privacy considerations must be accounted for (e.g. privacy notifications, breach investigation) and other potentially affected customers must be notified. The vendor should provide information needed for proper incident response to enable successful breach determinations.

If the complaint is associated with vendor managed or owned assets but not a vendor product, such as a service laptop or removable media, then upon receiving the complaint the vendor will inform its information security organization. Depending on the type of incident, notification of privacy or compliance officers may be needed as well. Additional responses may also be needed that include customer or regulatory notification.

Risk assessment and remediation planning is an integral part of the complaint investigation. As a part of this assessment, product cybersecurity risks are documented in service and support complaint handling systems in addition to risk management files. Remediation may include advised compensating controls and fixes as appropriate.

ii. Reporting Considerations

In the interest of strengthening cybersecurity within the medical technology ecosystem, it is essential for vendors to communicate cybersecurity vulnerabilities to appropriate stakeholders. In addition to vendor customers, these stakeholders include Cyber Emergency Response Teams (CERTs) and groups that share medical technology vulnerability and threat information (e.g. information sharing and analysis organizations).

`

Vendors should also be aware of any additional reporting and remediation requirements imposed by regulators in the jurisdictions in which they operate (e.g. FDA guidance on Postmarket Management of Cybersecurity in Medical Devices for medical device manufacturers marketing product in the US), as these vulnerabilities may pose patient safety concerns.

iii. Security Incident Management, Response and Communication

Provide timely responses and communications to all stakeholders impacted by vulnerabilities and incidents for commercialized products as described below.

- Manage internally reported issues within 30 days of initial discovery and the designated cross-functional team provides an update of the issue status to internal stakeholders and governance every 60 days thereafter until closure.
- Produce targeted customer bulletins or notifications and post to a public webpage or deliver via other available mechanisms to customers within 30 days of initial discovery for customer and third-party reported issues. Evaluate related customer security documentation to determine if updates are indicated; if deemed necessary, proceed to update. Provide status updates to customers and third-parties reporting vulnerabilities and incidents with a routine cadence established by the cross-functional team while complaint handling investigation is in progress. Achieving the aforementioned timing for bulletins or notifications by the vendor during incidents may be dependent on timely and accurate communication with customers.
- Coordinate vulnerability disclosures with a Cyber Emergency Response Team (CERT) and Information Sharing and Analysis Organization (ISAO) recognized by the FDA. For an overview of vulnerability disclosure terms, definitions, concepts, guidelines, and benefits please see the international standard and white paper referenced under "Security Incident Response and Communication" in Appendix D. Though out of scope for this document, other reporting such as that required by federal (e.g. the Health Insurance Portability and Accountability Act (HIPAA)) and state laws, regulatory compliance etc. may be needed. Figure 4 below is an example of a coordinated vulnerability disclosure process.

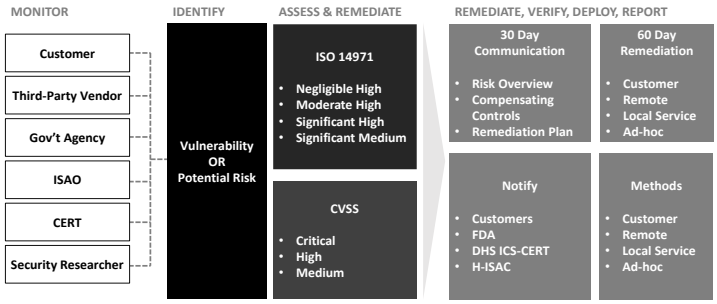

Figure 4. Example coordinated vulnerability disclosure process. Organizations obtain vulnerability information by monitoring various sources. Subsequently a potential vulnerability is identified, assessed, verified, remediated, and communicated as appropriate.

iv. Remediation Planning

Throughout design and development, a product security risk assessment is necessary to determine the level of risk and subsequent actions for security requirements including remediation planning. Below is an example of how low, medium and high risks can be managed.

- Low risk can be addressed or accepted as is and documented as an exception (see following section to learn more about exceptions)
- Medium to high and critical risk can be addressed as requirements for design input and mitigated accordingly
- Routine vulnerability and patch management may be addressed continuously

For commercialized products, security risk assessment and remediation planning is performed as part of a post market management (post-launch) process.

- Low risks may be addressed separately in a reasonable amount of time, but at minimum during the next product or software update
- Recommendations for medium to high and critical risks, which may align with uncontrolled risks per FDA's guidance Postmarket Management of Cybersecurity in Medical Devices, include communicating with the customer and user community about the vulnerability, identifying the devices which could potentially be impacted and providing interim control measures to mitigate risk as well as a remediation plan within 30 days of learning of the vulnerability. Patches must be available with at least one of the deployment methods promptly and within a maximum of 60 days after learning of the vulnerability. As soon as possible but no later than 60 days after learning of the vulnerability, the manufacturer fixes the vulnerability, validates the change, and distributes the deployable fix to its customers and user community such that the residual risk is brought down to an acceptable level.
- Risks which have resulted in an incident where unauthorized disclosure of PHI or PII will require data breach investigation and potential notification to customers in accordance with local laws and regulation. Other sensitive information and data such as intellectual property will require data breach investigation and potential notification to stakeholders.

Corrective and preventive action plans (CAPA) are established in compliance with vendor CAPA policy/procedure in order to evaluate the need to correct existing or potential quality issues that impact the security of products and to develop actions to prevent their occurrence or recurrence.

v. Exceptions

An exception is an instance when a cybersecurity risk is identified (both pre- and post-launch of the product) and the vendor determines that no action is needed. As is appropriate in all cases, it is important for the manufacturer to document the risk in the product's design history file and/or risk management files. For risks documented as exceptions that require compensating controls to reduce the risk to none-to-low risk, a description of the risk and the compensating controls, including associated procedures, should be provided in customer security documentation for the product.

vi. Vulnerability Management and Patch Management

`

Prior to commercialization, a vendor establishes a cybersecurity management plan to identify, evaluate, and respond to any cybersecurity incident or vulnerability including known and zero-day vulnerabilities. The plan would not be complete without addressing routine patching throughout the product lifecycle. Standardizing a pre-determined frequency for patches and updates is recommended, with a quarterly frequency at minimum. Publishing and coordinating patches in a timely manner so as to mitigate medium to high risk vulnerabilities is of prime importance to any vulnerability and patch management program. Critical elements of a vulnerability and patch management plan include the ability to:

- Continuously monitor, track, and plan for cybersecurity incidents, vulnerabilities, upstream patches, and end of support dates from predefined sources based on inventory of firmware, software, communication modules, etc. Products and components (including those contracted components provided by third-party entities) may also be a source of vulnerabilities and should similarly be subject to monitoring
- Determine the level of risk and subsequent actions necessary to mitigate cybersecurity risks by using product risk assessment, remediation planning and product security risk assessment. In particular, document cybersecurity risks in defect, bug, or issue tracking systems or product backlog, in addition to design history files and/or risk management files
- Validate the remediation and successful patching of vulnerabilities, including impact to performance and clinical use
- Perform proper version controlling to ensure patches can be identified once deployed on products
- Identify capabilities necessary for customers and vendors to determine if a security incident has occurred from any exploited vulnerability
- Deploy remediation, including routine and emergency software patches, by implementing at least one of the following secured methods that are then documented by both vendor and customer:
    - Remote Update: Patches applied via secure authorized remote service and support platforms provided by the vendor
    - Customer Administered: Validated patches will be made available for customer retrieval and installation from a designated source including direct download from the third-party that provides the product or component
    - Service Visit: Local service administered cybersecurity patches. Note that this method is less optimal due to the time required to deploy local service personnel to customer facilities. However, it has utility in cases where faulty patching has foreseeable and serious safety risk and local service personnel may be required for resolution
    - Ad-hoc Patching: Customers may accept engineering and technical risk for all other deployment mechanisms and/or application of cybersecurity patches not validated by the vendor. Note that this method is not advised due to the lack of validation by the vendor and potential impact to system performance or patient safety

`

- Make customers aware of the availability of cybersecurity patches and upgrades for products through a public webpage and/or direct customer notification (e.g., email followed by letter).
    - For vendor-managed remote updates and service visits, routine reporting to customers of failures to patch products in the field is necessary, including products and components provided by third-party entities that are no longer supported by their vendor
    - It is essential that customers establish processes and/or technical means for routinely monitoring the designated communication channels predefined by the vendor for new information or changes regarding patches

vii. End of Life/ End of Support and Decommissioning

The cybersecurity management plan incorporates consideration for appropriate actions for the vendor and its customers when security for the product can no longer be supported or when the vendor discontinues support and maintenance of the product.

- Consideration for end of support includes when third-party products and components are no longer supported by their manufacturer or developer and when known common vulnerabilities and exposures are identified but not remediated by the third-party component manufacturer or developer. Provide anticipated end of life and end of support dates to customers as part of customer security documentation.
- For commercialized products that will receive an end of life or end of support date for the first time, a reasonable amount of advanced notification is recommended so that customers can take any necessary action including removal of network connectivity, transition to a supported product, and implementation of compensating controls provided by the vendor as part of end of life and end of support. At a minimum, 3 years is considered a reasonable amount of time between communicating and making effective end of life or end of support.
- Customers should be aware of the end of life and end of support dates for systems in their inventory and make risk-based decisions on their replacement or continued use. If intending to replace, organizations can develop replacement/upgrade plans for each system. If the decision is continued use beyond the end of life and end of support dates, the customer is advised to perform a risk assessment to determine risk reduction strategies it can perform independently, which may include network segmentation, isolation, system hardening, or other defense-in-depth strategies.

VIII Evaluating JSP Progress and Maturity

A. Evaluating Progress

An organization involved in the design, development, production, deployment, service, and support of medical device and healthcare information technology may establish means for achieving each of the applicable plan components with target dates and periodically assessing progress and maturity against the JSP. The table below is an example of a JSP maturity assessment. Once the framework is understood, it is recommended that an initial assessment is

completed and the follow-ups scheduled and executed. Note that other maturity assessments may be of value and additional information on the CMMI maturity assessment is found in Appendix K.

Plan Component	Description	Current Maturity	Target Maturity	Milestones
Organization				
Structure	Does the organization have a Chief Product Security Officer? Does the organization have a product security function? Are the product security functions roles & responsibilities clearly defined? Is the product security function staffed appropriately?	[1-5]	[1-5]	[YYYY/MM]
Governance	Are there existing policies and/or procedures that cover product security? Has organizational leadership approved of the product security policy and procedures? Is the organization audited against product security policies/procedures? How frequently? Are product security metrics briefed to leadership such as Chief Quality Officer, Chief Medical Safety Officer, R&D leadership, etc.? If so, how frequently?			
Risk Management				
Risk Register	Has an inventory of products been created for	[1-5]	[1-5]	[YYYY/MM]

	commercialized products and products in development? Are security risks tracked in R&D defect tracking systems, design history or risk management files? Are security risks tracked in service complaint handling systems or risk management files?			
Risk Assessment	Is there an established method used for security risk assessment? Have policies and procedures been updated to incorporate security risk assessment and triage to other types of risk assessment?			
Supply Chain	Are development and manufacturing environments assessed and managed for adherence to information security policy?	[1-5]	[1-5]	[YYYY/MM]
Third-Party Entities	Have third-parties been assessed against the components of this framework? Are third-parties routinely assessed for security? Does the organization have security requirements in the contract language for suppliers and third-parties?			
Exceptions	Are exceptions to framework components documented in design history and/or risk management files? Are compensating controls associated with exceptions provided in customer security documentation?			

`

Design Control				
Design Input Security Requirements	Are cybersecurity requirements incorporated in design input for products in development?	[1-5]	[1-5]	[YYYY/MM]
Standards and Testing	Are system hardening standards, system patching, and vulnerability scanning incorporated in product development practices? Are secure coding standards and code analysis incorporated in product development practices? Is security testing such as penetration testing performed by trained cybersecurity professionals during design control? Is robustness testing performed during product development?			
Vulnerability Management & Patch Management	Have processes been instituted to monitor, identify, assess, remediate, and validate security patches for product software and third-party components? Are validated patches deployed using an established method? Can reports be generated to show patching failures? Is there a public webpage where customers can go to identify new patches?			
Customer Requirements	Do service and support personnel have procedures for requesting access to customer			

	systems and restoring security measures? Are controls in place for service personnel to uniquely authenticate to customer systems? Is there established policy and procedures around the use of removable media with products and handling of customer data?			
Cybersecurity Management Plan	Are plans in place to maintain security throughout the lifecycle of a product? Do products have anticipated end of life and/or end of support dates established with consideration to supporting third-party products and components?			
Complaint Handling				
Customer Complaint Escalation	Do escalation procedures define cybersecurity signals? Are customer reported cybersecurity issues documented in complaint handling systems? Are processes in place to ensure review of reported complaints related to cybersecurity?	[1-5]	[1-5]	[YYYY/MM]
Reporting Considerations	Have processes been established to notify a CERT, ISAO, and/or regulator as appropriate of reported cybersecurity issues?			
Security Incident Management, Response and Communication	Are internal teams engaged within 30 days of a reported security incident and updated every 60 days thereafter?			

`

	Are the incident response processes regularly practiced? Is there a public webpage where bulletins or advisories relating to vulnerabilities or incidents can be posted?			
Remediation Planning	Are there clearly defined criteria for remediation of security risk for products in development? Are there clearly defined criteria for remediation of security risk for commercialized product? Are medium to critical vulnerabilities communicated to customers within 30 days? Are medium to critical vulnerabilities remediated within 60 days?			

B. Maturity Levels

The following levels are used to describe the state of maturity for individual components of the Joint Security Plan. In order to move to a higher maturity level, all the elements of previous levels should be satisfied.

Level 1: Initial

One or multiple framework components have been presented to internal stakeholders and plans have been drafted, but there is no proven or formalized process nor people responsible.

Level 2: Managed

Framework components have been planned and execution is underway. The established plans ensure framework components are performed, measured, and controlled with routine visibility provided to management.

Level 3: Defined

All of the framework components have been achieved. Formal policies and procedures have been established as well as incorporated in quality management systems. Internal stakeholders have been provided clear description of activities and are provided training. Deliverables for the framework component are well documented and routinely reviewed among internal stakeholders.

Level 4: Quantitatively Managed

All aspects of a framework component are achieved and various performance metrics are collected to determine areas of improvement. The following are performance metrics that may be considered:

- Number of reported security complaints
  - Average response time to customers
  - Average time to closure for security complaints
  - Average time to customer communication
- Number of cybersecurity defects out of design control
  - Average time to remediation
- Percentage of patches successfully applied remotely to deployed product
- Percentage of patches successfully applied by customers to deployed product
- Percentage of patches successfully applied by service to deployed product

Level 5: Optimizing

Metrics collected on a framework component are routinely reviewed and process improvement plans are established. Quantitative process improvement objectives are established and continuously revised to reflect changes to industry standards and the JSP. Review of quantitative analysis produces predictable results. Process variation across multiple products is understood and when variation produces under-performance it is addressed through the creation of process improvement plans with cross-functional ownership. The process of continuous improvement is intrinsic to all those involved in the design, development, production, deployment, service, and support of medical device and healthcare information technology.

Appendix A: Acronyms

This appendix section provides an overview of the acronyms used in this document.

C-I-A	Confidentiality Integrity Availability
CISO	Chief Information Security Officer
DHS	U.S. Department of Homeland Security
EHR	Electronic Health Record
EU	European Union
FDA	U.S. Food and Drug Administration
GDPR	General Data Protection Regulation
HDO	Healthcare Delivery Organization
HCIC Task Force	Health Care Industry Cybersecurity Task Force
HHS	U.S. Department of Health and Human Services
HIMSS	Healthcare Information and Management Systems Society

HIPAA	Health Insurance Portability and Accountability Act
HPH	Healthcare and Public Health
IT	Information Technology
ISAO	Information Sharing and Analysis Organization
ISAC	Information Sharing and Analysis Center
MDM	Medical Device Manufacturer
NIST SP	National Institute of Standards and Technology Special Publication
NIS	Network and Information Systems Directive (EU) 2016/1148)
H-ISAC	Health Information Sharing and Analysis Center
NCCoE	National Cybersecurity Center of Excellence
NSA	National Security Agency
PHI	Protected Health Information
PII	Personally Identifiable Information
R&D	Research and Development
SDL	Security Development Lifecycle
SDLC	Software Development Life Cycle
U.S.	United States

Appendix B: Terminology

Various cybersecurity and healthcare centric terms are used throughout this document. This appendix section provides an overview of what is meant by some of these key terms. Note that some of these terminologies and definitions were derived from authoritative sources listed in Appendix D which describes the drafting of the Joint Security Plan.

Code Analysis: Source code analysis is the automated testing of a program's source code with the purpose of finding faults and fixing them before the software is sold or distributed.

Common Platform Enumeration (CPE): An industry standard structured naming scheme for information technology systems, software, and packages.

Common Vulnerability Exposure (CVE): CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems

Common Vulnerability Scoring System (CVSS): A security industry standard for prioritizing the severity of security issues.

Compensating Controls: Alternative security controls employed by organizations in lieu of specific controls. These are controls that provide equivalent or comparable protection for organizational information systems and the information processed, stored, or transmitted by those systems.

Complaint Handling: Process for receiving, reviewing, and evaluating complaints.

Coordinated Vulnerability Disclosure: The process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders, including the public

Controlled Risk: Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device's particular cybersecurity vulnerability.

Critical Functions: Any product functionality which impacts the clinical safety or significantly disrupts the business operations of Customers.

Customers: Includes healthcare providers and patients.

Customer Complaint: Complaint means any written, electronic, or oral communication that alleges deficiencies related to the identity, quality, durability, reliability, safety, effectiveness, or performance of a medical device or health information technology after it is released for distribution.

Customer Incident: An occurrence from a customer's use of software, products or services that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Customer Security Documentation: Security information provided to customers to enable more robust risk assessments, identify configurable security controls, and allow them to better protect their systems.

Customer Security Requirements: A user, or potential user, of a system's functional and non-functional requirements that achieve the security attributes of a system.

Decommissioning: The first physical process in the disposition process and includes proper identification, authorization for disposition, and sanitization of the equipment, as well as removal of Patient Health Information (PHI) or software, or both.

Design: A process of defining the architecture, modules, interfaces and data for a system to satisfy specified requirements.

Design control: The application of a formal methodology used to conduct product development activities.

Design Input Requirements: The physical and performance characteristics of a product that are used as the basis for product design.

Dynamic Code Analysis: The testing and evaluation of a program by executing data in real-time. The objective is to find errors in a program while it is running, rather than by repeatedly examining the code offline.

End of Life: Indicates that the product is in the end of its useful life, as defined by the vendor, and a vendor stops marketing, selling, or making major design changes in sustaining the product.

End of Support: A point beyond which the product manufacturer ceases to provide support, which may include cybersecurity support, for a product or service.

`

Exceptions: An instance when a cybersecurity risk is identified (both pre- and post-launch of the product) and the vendor determines that no action is needed.

Failure Mode and Effects Analysis (FMEA): A step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.

Fuzz Testing: A software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems and is a type of robustness testing.

Harm: Injury or damage to the health of people, or damage to property or the environment.

Hazard: Potential source of harm.

Hazard Analysis: The first step in a process used to assess risk and used to identity different types of hazard.

Incident Response: Actions taken to mitigate or resolve a security incident.

Internal/External Security Audit: Review and examination of data processing system records and activities to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy, and procedures.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the data, applications, or operating system. This includes both known and unknown (Zero Day) viruses, spyware, ransomware, and other forms of malicious code that exploit vulnerable systems.

Patch Management: The systematic monitoring, identification, assessment, remediation, deployment, and verification of operating system and application software code updates. These updates are known as patches, hot fixes, and service packs to operating systems, third-party products and components, and in-house developed software.

Patient Harm: Physical injury or damage to the health of patients, including death. Cybersecurity exploits (e.g. loss of authenticity, availability, integrity, or confidentiality) of a device may pose a risk to health and may result in patient harm.

Patient Safety: The prevention of harm to patients including that which may occur from cybersecurity related events.

Penetration Testing: A test methodology in which assessors, using all available documentation such as system design and working under specific constraints, attempt to circumvent the security features of an information system.

Preliminary Hazard Analysis (PHA): A technique used in the early stages of system design. It focuses on identifying apparent hazards, assessing the severity of potential accidents that could occur involving the hazards, and identifying safeguards for reducing the risks associated with the hazards.

Product Lifecycle: Managing the entire lifecycle of a product from inception, through engineering design and manufacture, to service and disposal of manufactured products.

`

Product Security Risk Assessment: Overall process of risk analysis and a risk evaluation for security issues found in products using impact to confidentiality, integrity, and availability to patients, customers, and vendor to determine the acceptability of the risk.

Remediation: Countermeasures to reduce a cyber asset's susceptibility to cyber-attack over a range of attack tactics, techniques, and procedures.

Remediation Planning: Planning of processes and actions by which organizations identify and resolve threats to their system.

Remote Access: Access to a product or an organization's non-public information system by an authorized user such as Service and Support communicating through an external network.

Remote Support: Support activities conducted by individuals communicating through an external network (e.g., the Internet).

Removable Media: Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device and used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar USB storage devices.

Risk Management: Risk management is an integral part of the medical device product development lifecycle. It is a systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk.

Robustness Testing: A testing methodology to detect the vulnerabilities of a component under unexpected inputs or in a stressful environment.

Secure Coding Standards: Guidelines for writing software code that mitigates common security flaws specific to a programming language or in general to all software.

Security Incident: An event that may indicate that a device’s data and security may have been compromised. This includes, but is not limited to:

- Attempts to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware or software characteristics without owner’s knowledge, instruction or consent

Security Management Plan: Used to document all framework components carried out through the design process and post commercialization. May also capture technical and process gaps, including exceptions. May be incorporated in a product risk management file or equivalent.

Security Requirements: A set of design-level requirements that comprise a product or other commercial offerings, ensure security issues are mitigated in both software and system components during design control, and are processed through Risk Management.

Sensitive Information and Data: Protected health information (PHI), personally identifiable information (PII), proprietary software source code or business logic, configuration parameters, user credentials, cryptographic keys, quality control and calibration results.

Static Code Analysis: The automated analysis of software code for security flaws and adherence to a secure coding standard.

System Hardening Standards: A documented process or mechanism for securely configuring or implementing commonly used technologies.

Third-Party Entities: External individuals and organizations such as vendor and suppliers involved with products or acquisition, that collaborate at any point in the product lifecycle, including acquisition, development and servicing.

Threat Modeling: Structured activity for identifying and managing threats.

Threat Monitoring: Solutions or processes dedicated to continuously monitoring systems, networks and endpoints for signs of a security threat such as intrusions or data exfiltration.

Threat Source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

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

Validation: Establishing by objective evidence that specified requirements conform with user needs and intended use(s).

Vendors: Includes medical device manufacturers and health IT vendors.

Verification: Confirmation by objective evidence that the results of the design effort meet the design input.

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Disclosure: Policy practiced by organizations as well as individuals regarding the disclosure or publishing of information about security vulnerabilities and exploits pertaining to a computer system, network or software.

Vulnerability Scanning: The automated analysis and detection of vulnerabilities such as missing patches and misconfiguration in operating systems and other third-party software.

Appendix C: Roles and Responsibilities

Numerous stakeholders may leverage and benefit from the security activities and processes described in this document. To provide additional context, the roles and responsibilities of these stakeholders are described in this appendix section.

For customer stakeholders

1. **Patients:** Review security documentation provided by vendors and healthcare providers for consumer products and in-home environments such that cybersecurity risks are understood and managed.
2. **Healthcare Providers:** Assess the risk of new information systems entering their facilities; manage risks over the lifecycle of these information systems, including monitoring of vulnerability disclosures, maintaining patches, securing network environments and enterprise systems; and provide training for their associates on their roles for managing cybersecurity. Also referred to as healthcare delivery organizations (HDOs).

For vendor stakeholders

1. **Medical Device Manufacturers:** Responsible for implementing security throughout the design, development, and complaint handling for medical devices. In addition, responsible for providing timely communication to customers in the form of product security documentation, vulnerability disclosures, and the availability of security patches.
2. **Health IT Vendors:** Responsible for implementing security throughout the design, development, and complaint handling for healthcare information technology. In addition, responsible for providing timely communication to customers in the form of product security documentation, vulnerability disclosures, and the availability of security patches.
3. **Product Security:** Creation and maintenance of policies, procedures, tooling, guidance, training and awareness for product security across business units and functions. Product security will support product security risk assessments, automated security testing, penetration testing, remediation planning services for R&D and complaint handling.
4. **Quality:** Ensures the framework is aligned and consistent with other corporate policies, as well as global regulations and standards for product development, risk management, manufacturing, and support. Quality, jointly with product security, will ensure adherence to the framework as with any other quality policy such as risk management and reporting requirements.
5. **Research and Development (R&D):** Responsible for incorporating security in budgeting and resource planning; provides technical information for product security risk assessment; establishes design requirements in the development process and throughout the product lifecycle including post-commercialization maintainability. R&D will maintain record of security defects in accordance with the business unit quality management systems including design control and risk management procedures.
6. **Product & Portfolio Management (PM, PPM):** Responsible for ensuring product security is incorporated in budget, resource, project, and roadmap planning activities throughout the product lifecycle.
7. **Complaint Handling Unit:** Responsible for identifying complaints that have a product security impact and proper escalation of complaints.
8. **Service and Support:** Ensure proper response to security incidents and events with products at customer sites, including proper documentation records as per business unit complaint handling procedures. Secure service assets, maintain validated security updates and ensure secure implementation, periodic reporting of security incident and events and security update tracking.
9. **Business Unit and Regional Leadership:** Responsible for communication, compliance and adherence of the framework at the regional and local business levels. This may include the creation of local policies that align with and supplement where needed due to regional laws and regulation the over-arching framework.
10. **Legal:** Provides business units with guidance on incident response, adherence to local security and privacy laws to ensure legal content meets policies.
11. **Privacy:** Ensures the appropriate protection of data, such as information from or about our employees, our customers, and users of our products worldwide.
12. **Regulatory:** Provides business units and product security with guidance on local security and privacy regulation, including any upcoming changes to those regulations.

`

13. **Information Security:** Ensures vendor managed assets, including but not limited to laptops, desktop computers, servers, removable media, and networks that interact with products align and adhere to the vendor information security policy.
14. **Third-Party Entities:** Adhere to requirements in the framework and vendor information security procedure. Document any exceptions in design history and/or risk management files.

Appendix D: Drafting of the Joint Security Plan

The intent and purpose of this appendix section is to outline and explain the drafting process and authoritative sources used to address traceability to US and International standards for the Medical Device and Health IT Joint Security Plan.

In November of 2017, with facilitation by the Healthcare Sector Coordinating Council (HSCC), an initial draft of the Joint Security Plan was developed by a group of medical device manufacturers, health IT vendors, and FDA representatives.

In February of 2018, through the Health Information Sharing and Analysis Center (H-ISAC) and HSCC, a group of healthcare providers was invited to participate in the drafting process of the Joint Security Plan.

Following the review by medical device manufacturers, health IT vendors, and healthcare providers, the HSCC invited government and policymakers to provide feedback and promote use of the Joint Security Plan among all stakeholders referenced in the document.

There are many different authoritative sources which were used to develop and/or can be used to achieve aspects of the Joint Security Plan. The following is a list of those sources and the associated section in the Joint Security Plan:

JSP Framework Overview	
Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication	https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
Risk Management	
AAMI TIR 57	http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729
IEC 80001-1	https://www.iso.org/standard/44863.html
NIST CSF	https://www.nist.gov/cyberframework
An Introduction to Computer Security: the NIST Handbook	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-12.pdf

ISACA Risk IT Framework for Management of IT Related Business Risks	http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx
ISO 14971:2007 Medical devices -- Application of risk management to medical devices	https://www.iso.org/standard/38193.html
Risk Assessment	
Common Vulnerability Scoring System	https://www.first.org/cvss/user-guide
NIST Special Publication 800-30 Revision 1.0 2012 Guide For Conducting Risk Assessments	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
Design Control	
Content of Premarket Submissions for. Management of Cybersecurity in. Medical Devices	https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	https://standardscatalog.ul.com/standards/en/standard_2900-1_1
UL 2900-2-1 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems	https://standardscatalog.ul.com/standards/en/standard_2900-2-1_1
NIST SP 800-160 Systems Security Engineering. Considerations for a Multidisciplinary Approach in the. Engineering of Trustworthy Secure Systems	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
Catalog of Control Systems Security: Recommendations for Standards Developers	https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf
Secure Architecture Design	https://ics-cert.us-cert.gov/Secure-Architecture-Design
NIST Cybersecurity Practice Guide SP 1800-8, Wireless Infusion Pumps	https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8a-draft.pdf
NIST SPECIAL PUBLICATION 1800-8B Volume B:	https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8b-draft.pdf

`

Approach, Architecture, and Security Characteristics	
Secure Software Development Life Cycle Processes	https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes
OWASP Security By Design Principles	https://www.owasp.org/index.php/Security_by_Design_Principles#Security_principles)
Standards and Testing	
DISA Security Technical Implementation Guides	https://iase.disa.mil/stigs/Pages/a-z.aspx
NIST Checklists	https://www.nist.gov/programs-projects/national-checklist-program
NSA Guides	https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/
CIS Benchmarks	https://benchmarks.cisecurity.org/downloads/benchmarks/
SEI CERT Coding Standards	https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards
OWASP Secure Coding Practices	https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
MS Secure Coding Guidelines	https://msdn.microsoft.com/en-us/library/fkytk30f(v=vs.110).aspx
Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Defense_in_Depth_Strategies_S508C.pdf
Vulnerability and Patch Management	
ISO/IEC 30111	https://www.iso.org/standard/53231.html
NIST National Vulnerability Database	https://www.nist.gov/programs-projects/national-vulnerability-database-nvd
CVE Details	https://www.cvedetails.com/index.php
Department of Homeland Security ICS-CERT Division	https://ics-cert.us-cert.gov/advisories
Carnegie Melon University Software Engineering Institute	https://www.kb.cert.org/vuls/
Guide for Cybersecurity Event Recovery	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

`

SANS Vulnerability Management	https://www.sans.org/reading-room/whitepapers/projectmanagement/building-vulnerability-management-program-project-management-approach-35932
Customer Security Documentation	
HIMMS/NEMA Manufacturers Disclosure Statement for Medical Device Security (MDS2)	http://www.himss.org/resourcelibrary/MDS2
Software Identification Tags (SWID)	https://nvd.nist.gov/products/swid
Common Platform Enumeration (CPE)	https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe/
Reporting Considerations	
Postmarket Management of Cybersecurity in Medical Devices	https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
Security Incident Response and Communication	
ISO/IEC 29147	https://www.iso.org/standard/72311.html
Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure	http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf
Evaluating Joint Security Plan Progress and Maturity	
Capability Maturity Model Index	http://cmmiinstitute.com/capability-maturity-model-integration
Cyber Threat Source Descriptions	https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
Overview of Cyber Vulnerabilities	https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

1017

United States of America	
21 CFR 806	https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=806&showFR=1
HIPAA – HITECH	https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
National Infrastructure Protection Plan (NIPP)	https://www.dhs.gov/cisa/national-infrastructure-protection-plan

`

European Union	
93/42/CE	https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF
EU General Data Protection Regulation (GDPR)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
Medical Device Regulations (MDR)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2017:117:TOC
Network and Information Systems (NIS) Directive	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
Canada	
The Personal Information Protection and Electronic Documents Act (PIPEDA)	https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Appendix E: Example Design Input Requirements for Security

The controls and features included in device design are informed by the device type, design, use environment, and intended use or functionality. As such, there is no one size fits all set of design inputs that should be utilized. Design inputs highlighted here in this appendix section are not intended to be comprehensive; rather, they serve as examples of input requirements that could be considered within the context of use for a given device. These design input requirements are categorized by OWASP Security Design Principles.

- **Minimize Attack Surface**
    1. The system shall restrict access of removable media to what is necessary for intended use.
    2. Execution of software on the system shall be restricted to explicitly authorized or validated software components.
    3. The system shall provide capability to anonymize exported data such that an individual or customer is not identifiable.
    4. Ports, protocols, services and addresses available on the system and its network connection shall be restricted to the minimum necessary for intended use and configurable locally by authorized user.
    5. The system shall be capable of enabling and disabling particular protocol stacks, individual ports and services, and contains manageable host-based firewall.
    6. The system shall provide capability to explicitly enable or disable remote access to the system.

7. The system shall notify users to change default passwords after initial use.
8. The system shall be capable of restricting repeated and failed user access attempts.

- **Establish Secure Defaults**
  9. The system shall have the ability to require a minimum password length.
  10. The system shall have the ability to require a minimum password complexity.
  11. The system shall have the ability to require periodic password renewal.
  12. The system shall have the ability to restrict password reuse.
  13. The system shall have the capability to automatically or manually back-up data necessary for intended use locally or to an external location.
  14. All sensitive information and data shall be encrypted in transit and at rest using an industry-accepted encryption mechanism and practice.
  15. The system shall prominently notify users when sensitive information and data are displayed on screen or if encryption is disabled in transit.
  16. The system shall have routine functionality for handling exceptions, errors and aborts that does not expose sensitive information and data.
  17. The system shall enforce strict order of execution during system start and end.
  18. All remote or local user activity which interacts with sensitive information and data as well as critical functions on the system shall be recorded in an audit log.
  19. All audit log entries shall include a start and end date-timestamp, user ID, role/privileges at time of access, success/failure and a description of the action performed.
  20. The audit log shall locally retain an individual entry for a configurable period of time or allocation of file system space.
  21. The system shall provide capability for a user to reset their own password or administrative reset, which is logged.
  22. The system shall provide the ability to create and assign a unique user ID and password to each remote or local user.
- **Principle of Least Privilege**
  23. Execution of software on the system shall be limited to the minimum privileges necessary.
  24. The system shall support the creation and assignment of roles that grant the minimum user privileges necessary for intended use of data and functions.
- **Principle of Defense in Depth**
  25. The system shall support multiple factors for user authentication and capable of centralized authentication.
  26. The system shall provide capability to prevent the execution of known malicious software.
  27. The system shall be capable of manually or automatically locking the display and requiring user authentication after a configurable period of user inactivity in order to continue use such that sensitive information and data are not visible.
  28. The system shall provide capability for a user to reset their own password or administrative reset, which is logged.
- **Fail Securely**
  29. The system shall be capable of restoring functionality to an operational state.

`

- **Don't Trust Services**
    30. The integrity and composition of all data as input or output of the system shall be validated such that modification is detected and/or rejected.
    31. All remote or local access to the system by user or an external system shall be authenticated prior to granting access to data or functions.
- **Separation of Duties**
    32. The audit log shall be restricted in access to only authorized users.
    33. The audit log shall be exportable and readable by authorized users and have the capability to integrate with security information and event management for real-time analysis.
- **Avoid Security by Obscurity**
    34. The security of a system shall not rely upon knowledge of the source code or shared hard coded credentials being kept secret.
- **Keep Security Simple**
    35. The system shall allow security controls to be configured with no significant downtime and centrally managed by authorized users.
- **Fix Security Issues Correctly**
    36. The system shall support authorized updates to mechanisms for controlling the execution of authorized or malicious software.
    37. Components of the system shall support software updating and patches with no significant downtime using standard centralized patch management systems.

Appendix F: Example Third-Party Security Agreement

It is important for vendors to consider the security of various components in their supply chain at the time of procurement. This appendix section specifies security requirements applicable to third-party suppliers that provide product development and post-market product management services to a given vendor.

The supplier is responsible for understanding the risk of [Company] and [Company's] customers' information and products it will access, process, manage, or store in the performance of services to [Company], and [Company's] customers. Compliance with the Association for the Advancement of Medical Instrumentation's (AAMI) "Technical Information Report (TIR) 57 - Principles for medical device security—Risk management" is recommended for meeting these objectives.

1. **PRODUCT DEVELOPMENT**
    1.1 Cybersecurity requirements are evaluated and documented during product design.
    1.2 Cybersecurity threats and risks are evaluated and documented as part of a risk analysis process during product design.
    1.3 Cybersecurity testing is completed as a part of verification and validation activities. Testing includes, but is not limited to, the following:
        a) Vulnerability scanning
        b) Static/binary code scanning
        c) Fuzz testing
        d) Customized test cases to evaluate defined cybersecurity requirements

e) Penetration tests

1.4 Cybersecurity penetration test is performed before the product is launched.

1.5 Defects identified during security testing shall be documented and evaluated for correction based on risk analysis process.

1.6 A software inventory or bill of materials shall be documented identifying all software of unknown provenance (SOUP) and third-party software components in a device and any backend support and specialist development systems.

a) A security assessment of third party and SOUP components is performed to determine version and patches are up to date and existing vulnerabilities are evaluated for risk and corrective action.

b) At the request of [Company] product owners and stakeholders, documentation and/or evidence of the above shall be made available.

c) At the request of [Company] product owners and stakeholders, source code and or binary files shall be made available.

d) Licensing arrangements for third party software, that establishes permissions for use, longevity and liabilities shall be negotiated with [Company] prior to incorporating such code in code developed for [Company].

e) Code associated with open source licenses shall be carefully considered and declared to [Company] and be appraised for the potential for [Company] to declare or reveal associated intellectual property in the form of bespoke, contracted code, at any time in the future.

2. POST-MARKET PRODUCT MANAGEMENT

2.1 Operating procedures are documented and approved for addressing cybersecurity patching, updating and remediation.

2.2 A process is defined to facilitate ongoing product change management throughout the lifecycle of the device.

2.3 A separate testing environment is established for evaluation of patches and incidents, including necessary devices and connection to backend systems.

2.4 Security measures shall be reviewed including threats, breaches, user access, new vulnerability reports, assessment of risks and necessary responses, at least annually or when there is a material change in business practices.

2.5 Training materials and a training plan for administration of the system including security critical roles and functions shall be established.

2.6 Termination and transfer of people resources from system access, key system knowledge, and process responsibilities shall be accomplished through documented processes.

2.7 Product documentation that is publicly available shall be identified and documented at least annually.

2.8 A process for handling (investigating and remediating) potential vulnerabilities in products is defined.

2.9 An incident mitigation and response plan is developed, including a timeframe during which mitigation occurs.

`

2.10 Complaint handling systems include notification to [Company] product owner and [Company's] product security organization if a cybersecurity complaint is reported by a customer.

2.11 The [Company] product owner and [Company's] product security organization shall be immediately notified if a cybersecurity issue is identified in a product.

2.12 At the request of [Company] product owners and stakeholders, documentation and/or evidence of the above shall be made available.

Appendix G: Example Customer Security Documentation

Customers require security documentation to enable more robust risk assessments, identify configurable security controls, and allow them to better protect their systems. This appendix section provides an overview of items that may be included in Customer Security Documentation. The following are examples of the types of information which may be included in documentation of security for medical devices or health IT:

- Product Description
- Hardware Specifications
- Operating Systems
- Third-party Software
- Network Ports and Services
- Sensitive Information and Data Transmitted
- Sensitive Information and Data Stored
- Network and Data Flow Diagram
- Malware Protection
- Authentication
- Network Controls
- Physical Controls
- Encryption
- Audit Logging
- Remote Connectivity
- Service Handling
- End-of-Life and End-of-Support
- Secure Coding Standards
- System Hardening Standards
- Risk Summary
- Third Party Certification or Attestation
- Manufacturer's Disclosure Statement for Medical Device Security

Product Description

[Insert basic description of function or purpose of the product or solution. Photo is optional, but recommended.]

Hardware Specifications

[List hardware components and specs]

- [List]
- [List]

Operating Systems

[List hardware operating systems and versions]

- [List]
- [List]

Third-party Software

[Also referred to as a Bill of Materials (BOM), includes a list of third-party software and version numbers where applicable. Having a cybersecurity bill of materials will aid customers in mitigating cybersecurity concerns on their healthcare technologies and ultimately to the systems/networks these technologies are attached to. The following are example attributes that would enable customers to leverage a bill of materials in protecting their assets.

Detailed attributes include:

• All commercial, open source, and custom code must be included

• Commercial technology components (e.g. processers, network cards, sound cards, graphic cards, memory) must be included

• The software list will be codified using an industry standard, such as Common Platform Enumeration (CPE), Software Identification tag (SWID), or Software Package Data Exchange (SPDX) that allows the software list to be searched and used to check against vulnerability feeds

• The list will be available in an electronic format that allows bulk uploading into common asset inventories, vulnerability management systems and configuration management databases.

• The BOM will be provided to a customer both upon a purchase and after significant software or hardware upgrades

• Vendors will maintain a BOM for all product versions that will be accessible remotely by customers]

Vendor and Name	Version	Description
[e.g. Microsoft Windows 10]	[e.g. 1607]	[e.g. Long Term Servicing Branch]

Network Ports and Services

[List Network Ports and Services]

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
XXX	XXX	XXXXX	XXXXX	XXX	XXX

Sensitive Information and Data Transmitted

[List sensitive information and data transmitted. This can include PHI/PII/Potential access to wireless credentials, etc.]

- [List]
- [List]

Sensitive Information and Data Stored

[List sensitive information and data stored. This can include PHI/PII/Potential access to wireless credentials, etc.]

- [List]
- [List]

Network and Data Flow Diagram

[Provide a diagram that describes how the product resides in a customer environment, showing the system components (1 or N computers, routers, switches, adjacent systems, remote connectivity) types of connectivity (e.g. RS232, RJ45, Serial to TCP/IP conversion), what types of data is in transit and at rest (e.g. PHI, QC, config data), and how these are secured (e.g. in transit IPSec, HTTPS/TLS, WIFI WPA2PSK; at rest BitLocker, SQL TDE)

Important: include if the device makes PHI/PII available via network or point-to-point connection (wired/wireless)?

- Is connected data encrypted in transit?
- Does service have network or p-to-p access to PHI (remote or in-room)?]

Malware Protection

[Describe and recommend the anti-malware measures available (e.g. validated AV solutions, AV partners, how AV is managed, application whitelisting like AppLocker or McAfee Embedded Control, advanced antimalware solutions, software restriction policies)]

Patch Management

[Describe and recommend the method in which we maintain, provide and deploy patch updates for this product. Examples include, “Patches are installed by a field service engineer during a routine service visit or during the yearly service visit. In the even that there is no patch management solution in place, also communicate this in this section.]

Authentication & Authorization

[Describe and recommend the controls that customers have with user’s authenticating and granting permissions to features and functionality, how users are managed, the default use accounts on the system and how to change and configure accounts. This includes the ability to disable user accounts]

Network Controls

`

[Describe and recommend the firewall rules, IPSec rules, host file restrictions, browser Internet access restrictions, MAC and IP address filtering)]

Encryption

[Describe and recommend where and how encryption is applied on the system (e.g. all network traffic is TLS 1.2, at rest is BitLocker with AES 256)]

Audit Logging

[Describe the audit logging process, where they are stored, what an auditable event entails, who has access to audit logs and any file permissions. Describe if audit logs are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC).

- What is the typical and maximum number of records retained on the device when in use?
- Do users have a means to irreversibly delete audit log records in the device?
- Does Service ever retain copies of PHI/PII data (is it encrypted by service) in audit logs?
- Application Auditing
    - Audit file location: E:\PieRoot\Logfiles*.pld
    - Audit files hashed with SHA256 when complete for integrity.
    - Auditable Events:
        - Service Start/Stop
        - User login/logout
        - User session created/destroyed.
        - User login from multiple workstations.
        - Client application connect/disconnect with IP address and port.
        - Failed client connection attempts.
        - Changes in application configuration.
        - Failed/successful attempts to access, modify, or delete security objects; e.g. roles, permissions, etc.
- Audit file permissions:
    - Administrators group: Read.
    - Auditors group: Read.
    - DB Auditors group: Full control.
    - DB Administrators group: Full control.
    - Virtual/Managed service accounts (audit file creators): Full control.
    - Users: None.]

Remote Connectivity

[Describe the nature of remote connectivity, what ports, protocols, URLs and endpoints for communication as well as security measures applied to the remote connection (e.g. TLS)]

Service Handling

[Describe what routine maintenance service personnel perform, what security policies and procedures they follow (e.g. never take PHI or PII, on-site authorization protocol, encrypted Removable Media, hardened service laptops, whether or not service laptops connect to product,

`

routine AV update during visit, secure installation/implementation principles, service authentication to product, decommissioning process, once decommissioned how the product hard drive is wiped, how the product is recovered from the field or destroyed, and what customer data and features service personnel interact with)]

End-of-Life and End-of-Support

[Describe the life cycle of the product in relation to when it will no longer be sold, updated, and supported. Provide dates if available otherwise describe how EOL/EOS is communicated.]

Secure Coding Standards

[Describe the secure coding standards used]

- [List the industry secure coding standards used during software development (e.g. SEI CERT Java Secure Coding Standard)]

System Hardening Standards

[Describe the secure hardening standards used, may also create appendix to list out standards used.]

Name of Standard	Version Number	Source of Standard
[Insert name of standard]	[Insert version number]	[Insert URL]

Risk Summary

[This section should contain a summary of risks found within a penetration test, remediation report, or other topics and compensating controls that correspond to additional risks outlined in the product security white paper. This may also include any findings from application scans.]

Appendix H: Example Organizational Structure

The intent of this appendix section is to provide an example of roles and responsibilities within organizations to support the adoption and continuous improvement of cyber security for medical devices and health IT:

Medical Device Manufacturers and Health IT Vendors

- **Chief Product Security/Cybersecurity Officer:** Responsibility to drive product and solution security throughout a vendor organization including identifying best practices and companywide technical standards, processes, and policies, for overall governance or guidance. In addition, this individual will advise executive management, product management, project management, R&D heads and manufacturing heads with regard to security for all products, solutions and services. Responsible for implementing pre-market product security design and post-market support including cybersecurity events and incidents for products in scope. Independent of Information Security and in cooperation with the CEO, this individual will advise appropriate processes and structures to introduce security into products, solutions and services.
- **Product Security/Cybersecurity Engineering**

`

- Security Architects: This person will work with R&D, service, and quality organizations to research common security vulnerabilities and their remediation; develop procedures to incorporate hardening into product development; work with individual product teams in securing their products; and proactively educate teams across the company on security best practices for products under development.
- Penetration Testers: This person will perform security penetration testing, ethical hacking and red team activities in order to identify unique and common vulnerabilities in products under development. This includes performing vulnerability analysis and research, formalizing security testing procedures in the product lifecycle, performing penetration testing with remediation plans and formal reporting, and supporting red team, covert, and security activities to test organizational readiness.

- **Product Security/Cybersecurity Incident Response**
  - Incident Responder: This person will manage technical strategy, process, timelines, resources and progress for incidents relating to products at customer sites or with security researchers.
  - Vulnerability Manager: This person will track the escalation, follow-up, and remediation of vulnerabilities throughout the product lifecycle.
- **Product Security/Cybersecurity Program Management**
  - Policy and Compliance Analyst: This person will ensure the adoption and continuous improvement of security policies and procedures for products in compliance with industry standards and regulations.
  - Strategic Program Manager: This person will work cross-functionally to create programs and initiatives for establishing training, awareness, and fundamental capabilities for improving security of products.
- **Product Security Testing** – Responsible for assessing and testing products in development and in the market so as to understand cybersecurity risk and find issues before an external party does. Comprised of Product Security members and other participants (such as 3rd parties) as needed.

Larger organizations may choose to have multiple business or product-specific roles including a dedicated product security officer, manager, and/or engineers.

Healthcare Provider

- Healthcare providers may create similar organizational structures to align with vendors under a Chief Clinical Information Security/Cybersecurity Officer, with distinct consideration for the healthcare provider's specific needs relating to security during the procurement, operation, and decommissioning of medical devices and health IT products.
- A broad set of stakeholders should be involved including people from clinical practices, medical device support organizations and technology and security areas.

`

Appendix I: Example Organizational Training

The intent of this appendix section is to provide training information that will help organizations mature their cybersecurity programs. A comprehensive training program for cybersecurity includes the following:

- **Training Requirements**
  Requirements for training each relevant role must be established and periodically reviewed to determine if they need to be updated.
- **General Awareness Training**
  All relevant employees in the organization should understand the principles of cybersecurity, the framework of the organization's program and the different roles and responsibilities for cybersecurity.
- **Training by Roles**
  - Training for Security Practitioners
    - Engineers
      - Architecture: Security experts who participate in architecting products or contribute to the security architecture components of products should be trained in secure architecture principles and patterns.
      - Threat modeling and security risk analysis: Security experts who participate in threat modeling should be trained in the principles of threat modeling and the use of threat modeling tools, as well as methods of translating threats into a risk management framework.
      - Design: Security experts who participate in product design or contribute to the security design of products should be trained in secure design principles and patterns.
      - Testing: Security experts who perform or guide security testing of products should be trained in security testing methodologies, tools and interpretation of testing results.
      - Forensics and Incident Response: Security experts who evaluate evidence of security incidents should have training in security forensic analysis in addition to practical experience. Those who participate in the incident response process should be trained in that process and the theory of incident response, in addition to practical experience.
    - Penetration Testing: Penetration testers should have proper training in penetration testing techniques and tools as well as considerable practical experience before being qualified as a penetration tester for products.
    - Security Officers/Directors/Managers/Advocates/Champions: Non-technical security practitioners should be trained in the secure development lifecycle, the company's security framework and the company's quality system.
  - Training for Related Activities – Non-dedicated Practitioners
    - Software/firmware/hardware/systems engineers

        - Secure Coding standards: Engineers involved in developing code should be trained in secure coding standards.
        - Static and dynamic code analysis tools: Engineers involved in development and/or configuration management should be trained in the use and interpretation of automated code analysis tools.
    - Sustaining engineering (maintenance for vulnerabilities): Engineers and product managers involved in maintenance of commercialized products should be trained in the interpretation of vulnerability notifications and the steps necessary to respond to vulnerabilities identified in the products.
    - Risk managers: Risk managers should be trained on the incorporation and interpretation of security risks within the existing risk management framework.
    - Requirements engineers: Requirements engineers should be trained to be able to incorporate standard security requirements into risk catalogs as well as novel requirements identified during threat modeling.
    - Deployment engineers: Those responsible for deploying products in the field should be trained on adapting the products to the IT environment as well as configuring that environment, to match the security requirements specified for the products.
    - Support and service engineers: Support and service engineers should be trained to recognize, remediate and escalate security issues reported or discovered in fielded systems.
    - Information Security/IT/Systems Administration (infrastructure): Those responsible for defining and implementing the security infrastructure of the company's IT and physical environments should be trained in the access and protection requirements of secure development and manufacturing.
- **Periodic refreshers for awareness:** Employees who have participated in the overall awareness and more detailed training should be given periodic refresher training to remind them of the key elements of the previously acquired training.
- **Periodic updates for changes in threat landscape, technology, program:** As the threat landscape changes, as new technology is developed in cybersecurity and as the company's security program evolves, the training requirements and trainings themselves should be updated to stay in synchronization.
- **Qualification and Certification of Security Experts:**
    - Certification: Requirements for certification for security experts and practitioners should be established and upheld as minimum qualifications to participate in these activities. Certifications can be external and/or internal (based on completion and confirmation of an internal training regime).
    - On the job experience: Minimum requirements for actual experience practicing security activities should be specified for a person to be considered a security expert in a particular sub-role of expertise.
    - Mentoring and community: Participation in the community of experts within the company should be included as a requirement to be considered a security expert. This may include peer relationships as well as mentor-mentee relationships.

`

- Levels of expertise: Different levels of expertise should be defined by the degree to which a practitioner has achieved these aspects of qualification. The levels should correspond to minimum requirements for specific security-related activities. For instance, a penetration tester may be allowed to be the lead tester for a product only in the case of a minimum amount of time practicing as a penetration tester.

- **Drills:** Periodic drills should be exercised, in order to ensure the ability of practitioners to apply trainings. These may take the form of tabletop incident response drills or full-blown red team/blue team exercises.

Appendix J: Example Security Risk Assessment Methods

Common Vulnerability Scoring System Rubric for Healthcare

CVSS provides a way to characterize and assess the severity of a cybersecurity vulnerability, and the IT industry has used it effectively to manage system and software vulnerabilities for many years. The purpose of this appendix section is to provide additional healthcare context for end users and vendors that leverage CVSS as a part of their vulnerability assessment.

CVSS and its associated rubric and examples were developed for enterprise information technology systems and do not adequately reflect the clinical environment and potential patient safety impacts. As such, a CVSS supplemental rubric tailored to explicitly consider the clinical environment and potential impacts to patient safety is being developed in collaboration with subject matter experts across the medical device ecosystem. The intent is to use the rubric with CVSS to provide a consistent and standardized way to communicate the severity of a vulnerability between multiple parties, including the medical device manufacturer, hospitals, clinicians, patients, Department of Homeland Security (DHS), and vulnerability researchers.

The draft "Rubric for Applying CVSS to Medical Devices" is found at https://www.mitre.org/md-cvss-rubric.

Appendix K: CMMI® for Development

CMMI for development is a reference model that includes activities and best practices for developing products and services. There are 5 CMMI maturity levels from level 1 to level 5 and these maturity levels provide a means for organizations to assess and describe their performance. This appendix section provides an overview of these maturity levels which may also be found at https://cmmiinstitute.com/learning/appraisals/levels.

Maturity Level 1: Initial

At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment to support processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. In spite of this chaos, maturity level 1 organizations often produce products and services that work, but they frequently exceed the budget and schedule documented in their plans. Maturity level 1 organizations are characterized by a tendency to overcommit, abandon their processes in

a time of crisis, and be unable to repeat their successes.

Maturity Level 2: Managed

At maturity level 2, the projects have ensured that processes are planned and executed in accordance with policy; the projects employ skilled people who have adequate resources to produce controlled outputs; involve relevant stakeholders; are monitored, controlled, and reviewed; and are evaluated for adherence to their process descriptions. The process discipline reflected by maturity level 2 helps to ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans.

Also at maturity level 2, the status of the work products are visible to management at defined points (e.g., at major milestones, at the completion of major tasks). Commitments are established among relevant stakeholders and are revised as needed. Work products are appropriately controlled. The work products and services satisfy their specified process descriptions, standards, and procedures.

Maturity Level 3: Defined

At maturity level 3, processes are well characterized and understood, and are described in standards, procedures, tools, and methods. The organization's set of standard processes, which is the basis for maturity level 3, is established and improved over time. These standard processes are used to establish consistency across the organization. Projects establish their defined processes by tailoring the organization's set of standard processes according to tailoring guidelines. (See the definition of "organization's set of standard processes" in the glossary.)

A critical distinction between maturity levels 2 and 3 is the scope of standards, process descriptions, and procedures. At maturity level 2, the standards, process descriptions, and procedures can be quite different in each specific instance of the process (e.g., on a particular project). At maturity level 3, the standards, process descriptions, and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit and therefore are more consistent except for the differences allowed by the tailoring guidelines.

Another critical distinction is that at maturity level 3, processes are typically described more rigorously than at maturity level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. At maturity level 3, processes are managed more proactively using an understanding of the interrelationships of process activities and detailed measures of the process, its work products, and its services. At maturity level 3, the organization further improves its processes that are related to the maturity level 2 process areas. Generic practices associated with generic goal 3 that were not addressed at maturity level 2 are applied to achieve maturity level 3.

Maturity Level 4: Quantitatively Managed

At maturity level 4, the organization and projects establish quantitative objectives for quality and process performance and use them as criteria in managing projects. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality

and process performance is understood in statistical terms and is managed throughout the life of projects.

For selected subprocesses, specific measures of process performance are collected and statistically analyzed. When selecting subprocesses for analyses, it is critical to understand the relationships between different subprocesses and their impact on achieving the objectives for quality and process performance. Such an approach helps to ensure that subprocess monitoring using statistical and other quantitative techniques is applied to where it has the most overall value to the business. Process performance baselines and models can be used to help set quality and process performance objectives that help achieve business objectives.

A critical distinction between maturity levels 3 and 4 is the predictability of process performance. At maturity level 4, the performance of projects and selected subprocesses is controlled using statistical and other quantitative techniques, and predictions are based, in part, on a statistical analysis of fine-grained process data.

Maturity Level 5: Optimizing

At maturity level 5, an organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the variation inherent in the process and the causes of process outcomes.

Maturity level 5 focuses on continually improving process performance through incremental and innovative process and technological improvements. The organization's quality and process performance objectives are established, continually revised to reflect changing business objectives and organizational performance, and used as criteria in managing process improvement. The effects of deployed process improvements are measured using statistical and other quantitative techniques and compared to quality and process performance objectives. The project's defined processes, the organization's set of standard processes, and supporting technology are targets of measurable improvement activities.

A critical distinction between maturity levels 4 and 5 is the focus on managing and improving organizational performance. At maturity level 4, the organization and projects focus on understanding and controlling performance at the subprocess level and using the results to manage projects. At maturity level 5, the organization is concerned with overall organizational performance using data collected from multiple projects. Analysis of the data identifies shortfalls or gaps in performance. These gaps are used to drive organizational process improvement that generates measurable improvement in performance.

##