**[Device Name]**

**Security Operations Manual**

**[Insert device image (optional)]**

**Applies to [Enter relevant part number and version for the product and its software, as applicable]**

This document was prepared by [**department/role name**] of Stryker’s [**division name**] division. See section 3.1 below for contact information.

**Template Notes:**

* The template information in the header should be replaced with applicable identification information for the SOM being developed (number, name, version). Replace “Form” with “Manual.”
* Contact Product Security as needed for assistance with this template: [ProductSecurityTeam@stryker.com](mailto:ProductSecurityTeam@stryker.com).
* The template information in the header should be replaced with applicable identification information for the SOM being developed (number, name, version).
* Remove the “Stryker Confidential” footer information, as this is appropriate for the template but not the final SOM. Add any other footer information, as appropriate (e.g., “This document is intended for circulation to Stryker employees, contractors, and customers only.”).
* Adjust formatting as needed. Instructions/guidance in blue text should be removed after being put into effect.
* In cases where relevant information is provided to the customer in other documentation (such as the IFU), the SOM may include a reference to the other document rather than duplicating information.
* “Not applicable” may be typed in sections and subsections which do not apply. Where a section and all of its subsections do not apply, the subsections may be deleted.
* Items in brackets [ ] are intended to be replaced with information as described within the brackets.
* Update the Table of Contents after all other edits are complete to account for sections that have been added, removed, or moved to different pages.

**Table of Contents**

[1. PURPOSE 5](#_Toc59610132)

[2. DEFINITIONS 5](#_Toc59610133)

[3. PRODUCT DESCRIPTION 8](#_Toc59610134)

[3.1 Device and Manufacturer Identification (DOC-1, 2, 3, 5) 8](#_Toc59610135)

[3.2 Device Intended Use (DOC-6) 8](#_Toc59610136)

[3.3 Related Manufacturer Programs (DOC-8, DOC-9) 8](#_Toc59610137)

[3.4 System Characterization and System Assets 8](#_Toc59610138)

[3.5 System Security Context and Intended Environment (SGUD-4) 9](#_Toc59610139)

[3.6 Network, Data Flow Diagram (DOC-10) 9](#_Toc59610140)

[3.7 Setup of SaMD (DOC-11) 10](#_Toc59610141)

[4. MANAGEMENT OF PII and PHI (MPII-1) 10](#_Toc59610142)

[4.1 Authority to Collect PHI 10](#_Toc59610143)

[4.2 Purpose Specification for PHI Use 10](#_Toc59610144)

[4.3 PHI Data Quality and Integrity 11](#_Toc59610145)

[4.4 PHI Data Deletion and Minimization (SGUD-2) 11](#_Toc59610146)

[4.5 Legal Roles and Related Requirements for Privacy 11](#_Toc59610147)

[4.6 Handling of Patient Requests for their PHI Access 11](#_Toc59610148)

[4.7 Storage and Removal of PII (MPII-2) 12](#_Toc59610149)

[4.8 Transmitting, Importing/Exporting of PII (MPII-3) 12](#_Toc59610150)

[5. AUTOMATIC LOGOFF (ALOF-1, 2) 13](#_Toc59610151)

[6. AUDIT CONTROLS (AUDT) 13](#_Toc59610152)

[6.1 Device-Specific Audit Log Configuration (AUDT-1) 13](#_Toc59610153)

[6.2 Events and Attributes Recorded (AUDT-2, 3, 4) 13](#_Toc59610154)

[6.3 Audit Log Protection (AUDT-7) 14](#_Toc59610155)

[6.4 Log Export, Use, and Notification (AUDT-5, 6, 8) 14](#_Toc59610156)

[7. AUTHORIZATION (AUTH) 14](#_Toc59610157)

[7.1 Access Prevention (AUTH-1) 15](#_Toc59610158)

[7.2 Privilege and Access (AUTH-2, 3, 4, 5, SGUD-3, 3.1) 15](#_Toc59610159)

[7.3 System Use Notification 15](#_Toc59610160)

[8. CYBER SECURITY PRODUCT UPGRADES (CSUP) 15](#_Toc59610161)

[8.1 Secure Servicing and Security Upgrades Overview (CSUP-1) 15](#_Toc59610162)

[8.2 General Parameters for Updates (CSUP-7, 8, 9, 10, 11) 16](#_Toc59610163)

[8.3 Operating System Updates (CSUP-2) 16](#_Toc59610164)

[8.4 Driver, Firmware Updates (CSUP-3) 16](#_Toc59610165)

[8.5 Anti-Malware Software Updates (CSUP-4) 17](#_Toc59610166)

[8.6 COTS (non-OS) Updates (CSUP-5) 17](#_Toc59610167)

[8.7 Other Software Component Updates (CSUP-6) 17](#_Toc59610168)

[9. HEALTH DATA DE-IDENTIFICATION (DIDT-1) 17](#_Toc59610169)

[10. DATA BACKUP AND DISASTER RECOVERY (DTBK-1, 2, 3, 4, 5, 6) 18](#_Toc59610170)

[11. EMERGENCY ACCESS (EMRG-1) 18](#_Toc59610171)

[12. HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU-1, 2) 18](#_Toc59610172)

[13. MALWARE DETECTION/PROTECTION (MLDP-1) 18](#_Toc59610173)

[13.1 Support of Anti-Malware (MDLP-2) 19](#_Toc59610174)

[13.2 Other Compensation/Protection Controls (MDLP-3, 4, 5) 19](#_Toc59610175)

[14. NODE AUTHENTICATION (NAUT-1, 2, 3) 19](#_Toc59610176)

[15. CONNECTIVITY CAPABILITIES (CONN) 20](#_Toc59610177)

[15.1 Hardware Connectivity Capabilities (CONN-1) 20](#_Toc59610178)

[15.2 Communication Provisions (CONN-2, 3, 4, 5, 6, 7) 20](#_Toc59610179)

[16. PERSON AUTHENTICATION (PAUT) 21](#_Toc59610180)

[16.1 Password/ID Assignments (PAUT-1) 21](#_Toc59610181)

[16.2 User Account Management (PAUT-2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14) 21](#_Toc59610182)

[17. PHYSICAL LOCKS (PLOK-1, 2, 3) 22](#_Toc59610183)

[18. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) 22](#_Toc59610184)

[19. SOFTWARE BILL OF MATERIALS (SBoM-1, 3) 22](#_Toc59610185)

[19.1 SBoM Structure and Updates (SBoM-2, 4) 22](#_Toc59610186)

[20. SYSTEM AND APPLICATION HARDENING (SAHD) 23](#_Toc59610187)

[21. HEALTH DATA STORAGE CONFIDENTIALITY (STCF-1, 2, 3, 4) 24](#_Toc59610188)

[22. TRANSMISSION CONFIDENTIALITY (TXCF) 24](#_Toc59610189)

[23. TRANSMISSION INTEGRITY (TXIG-1, 2) 25](#_Toc59610190)

[24. REMOTE SERVICE (RMOT-1, 2, 3) 25](#_Toc59610191)

[25. SECURITY PROGRAM INTEGRATION 25](#_Toc59610192)

[25.1 Vulnerability Management 26](#_Toc59610193)

[25.2 Incident Response 26](#_Toc59610194)

[25.3 Security Testing 26](#_Toc59610195)

[25.4 Scanning 26](#_Toc59610196)

[25.5 Risk Management 27](#_Toc59610197)

[25.6 Training and Awareness 27](#_Toc59610198)

[26. SECURE DECOMMISSIONING 27](#_Toc59610199)

# PURPOSE

This Security Operations Manual (SOM) provides information that Stryker’s customers need to integrate a specific Stryker device or health IT solution into a customer’s IT network environment. It also supports a customer’s ability to perform risk management, to identify configurable security controls, and to better protect their systems.

**Note**: This Manual is aligned with the structure of the Manufacturer Disclosure Statement for Medical Device Security (MDS2 form) in order to provide the supplemental information which is requested in the MDS2 form. The Question IDs from the MDS2 form are incorporated in the section headers to enable traceability between this document and the MDS2 form. There is no SGUD (Security Guidance) section in this document, as the entire document is the security guidance.

If there are other SOM documents or related customer-facing documents for related products, for other versions of the same product, or for other audiences, consider adding a statement about the scope of this document relative to the others. Likewise, if there are ancillary components that the device may or may not be configured to work with (e.g., cloud-based support options, iPad app), the SOM should explain whether it was written to describe security details when the device is configured to work with those components, without those components, or for both cases.

# DEFINITIONS

Add, remove, or update terms and definitions as needed. Terms specific to the device should be added if they are not explained or defined in section(s) where they are used.

**AAMI – Association for the Advancement of Medical Instrumentation**: An organization for advancing the development, and safe and effective use of medical technology. AAMI publishes standards and technical reports related to various aspects of medical device development and use (e.g., AAMI TIR57). See [www.aami.org](http://www.aami.org/).

interface for computing that defines interactions between multiple software intermediaries.

**API – Application Programming Interface**: An interface for computing that defines interactions between multiple software intermediaries.

**COTS – Commercial off-the-shelf**: Software (or any other item) that is sold as a packaged solution which is then adapted to satisfy the needs of the organization purchasing the COTS. Some medical devices utilize COTS software in addition to or instead of software developed by the manufacturer. See third-party software.

**Customer**: The individual or organization responsible for procurement and operation of the device. See Owner and Operator.

**Device:** The item being integrated or used for a healthcare purpose. A Medical Device or other health IT product may be referred to as a Device or a Product in this document.

**DICOM (Digital Imaging and Communications in Medicine)**: Standard developed by NEMA and the American College of Radiology, used worldwide to store, exchange, and transmit medical images.

**FDA – U.S. Food and Drug Administration:** A federal agency of the United States’ Department of Health and Human Services. See [www.fda.gov](http://www.fda.gov).

**HDO – Healthcare Delivery Organization**: Also “Health Delivery Organization,” an organization or group of organizations that are involved with the delivery of healthcare services. A hospital is an HDO. If an HDO purchases and operates a Stryker device, the HDO is also the Customer, Owner, and Operator per the definitions of those terms.

**IEC – International Electrotechnical Commission**: A global organization whose work underpins quality infrastructure and international trade in electronic goods. IEC publishes thousands of international standards, including documents related to medical device software (e.g., IEC 62304). See [www.iec.ch](http://www.iec.ch).

**IFU – Instructions for Use**: Information provided by the manufacturer in document or electronic form, informing the user of a device’s intended purpose and proper use and of any precautions to be take.

**Integrator**: The individual or organization who installs and configures the device/system into the operator’s environment.

**ISAO – Information Sharing and Analysis Organization:** An ISAO is any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability (source: from NIST SP 800-150).

**ISO – International Organization for Standardization**: An international standard-setting body that promotes proprietary, industrial, and commercial standards, and publishes standards relevant for information technology, privacy, and security (e.g., ISO/IEC 27034). See [www.iso.org](http://www.iso.org).

**Manufacturer**: The entity (Stryker) that builds the device and sells it to the customer.

**MDR – European Union (EU) Medical Device Regulation of 2017:** The European Union regulation concerning medical devices. See <https://ec.europa.eu/health/md_sector/overview_en>.

**MDS2 - Manufacturer Disclosure Statement for Medical Device Security**: A form created by the National Electrical Manufacturers Association (NEMA), intended to be completed by a medical device manufacturer and provided to customers, giving standardized information on security and privacy control features (ANSI/NEMA HN 1-2019). See [www.nema.org](http://www.nema.org).

**Medical Device:** See the following sources if a precise definition is required: FDA, MDR (EU) 2017/745, ISO 14971:2007.

**NEMA – National Electrical Manufacturers Association**: See [www.nema.org](http://www.nema.org).

**NIST - National Institute of Standards and Technology**: A physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. NIST has published comprehensive standards for the selection, implementation, and risk management of security and privacy controls (e.g., NIST SP 800-53). See [www.nist.gov](http://www.nist.gov).

**Operator**: The person(s) using the device for its intended purpose. This term may also sometimes refer to the person or organization responsible for procuring the device (owner, customer).

**OSS – Open Source Software**: Third party software licensed under an OSS license, in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose as long as the license terms are adhered to.

**Owner**: See Operator and Customer.

**PHI - Protected Health Information**: Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media; or transmitted, or maintained, in any other form or medium (source: extracted from 45 CFR Section 160). Note: This is a subset of PII.

**PII - Personally Identifiable Information**: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity… and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (source: from NIST SP 800-122).

**Product:** See Device.

**SaMD - Software as a Medical Device**: Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (source: from International Medical Device Regulators Forum).

**SBoM – Software Bill of Materials**: For a specific device, a listing of all software components that are incorporated into the final product. The SBOM may be used to assist with operational security planning by the HDO.

**SIEM – Security information and event management**: Software products and services in which security information management and security event management are combined, providing real-time analysis of security alerts generated by applications and network hardware.

**SiMD - Software in a Medical Device**: Software which is incorporated in a Medical Device and which is required for the medical device to fulfill a medical function, and/or software which is used to drive or control a hardware medical device.

**SOM - Security Operations Manual**: A product-specific guide to the secure integration of a product into a customer IT network (this document).

**Third-party software**: Third party software is software not developed by Stryker, and for which Stryker otherwise does not have complete ownership. See COTS and OSS.

**User**: See Operator.

# PRODUCT DESCRIPTION

|  |  |
| --- | --- |
| **Manufacturer Name** |  |
| **Stryker Division** |  |
| **Address** |  |
| **Device Description** | This should match the wording used in the MDS2 form, question DOC-2. Include what the product is, what it is to be used for, and a basic characterization of the product type (e.g., software, embedded system, etc.) at an overview level. |
| **Device Model, Version** |  |
| **Manufacturer Contact Information** | Enter contact information appropriate for the division, or the corporate contact email [ProductSecurity@stryker.com](mailto:ProductSecurity@stryker.com). Include a statement something like the one below.  Additional information and contact links are available on Stryker’s Product Security webpage, <https://www.stryker.com/us/en/about/governance/cyber-security.html>. |

# Device and Manufacturer Identification (DOC-1, 2, 3, 5)

# Device Intended Use (DOC-6)

Copy and paste the original, complete Intended Use statement, and provide a reference to its source.

# Related Manufacturer Programs (DOC-8, DOC-9)

Edit or amend the statements below, as appropriate.

When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is conducted. Based upon this assessment Stryker determines if further actions are required like providing security updates and/or providing communication to the customer in a timely manner. Vulnerability information may also be requested from Stryker at any time.

Stryker participates in the **MedTech Information Sharing and Analysis Organization** (ISAO), a part of **AdvaMed** (Advanced Medical Technology Association).

# System Characterization and System Assets

Describe the system, including its major components, purposes, and methods of performing the functions required. Refer to or expand on the Device Description and Device Intended Use statements above in order to orient a reader more fully to the security context of the product and the content of the architectural diagram(s) below.

For connected products, consider including a list of the system’s physical and logical assets with sufficient detail to allow the HDO IT department to understand the components that need to be protected and that could introduce risk to the network. The description of assets should include any appropriate mechanisms to identify specific versions or loaded software of a particular copy of the system.

Note: The Software Bill of Materials (SBoM) is intended to be documented in section 19; the present section’s list of system assets should not duplicate the list of software components at the SBoM level of detail but should refer to section 19 as appropriate.

# System Security Context and Intended Environment (SGUD-4)

At a high level, describe the security model applied to the product, addressing general security-relevant features of the product. This is not intended to duplicate more detailed information that follows, but to orient a reader to the overall picture that will be elaborated upon in later sections. Example sentence: “The system consists of software loaded to a general-purpose computer that inherits the security protections applied to the general-purpose computer.”

State at a high level the recommended compensating controls to put in place (e.g., “Controls have been built into the device as described in this document. It is also recommended that the customer utilize [control item, such as malware] as described in section(s) [section numbers].”).

Summarize and/or reference other SOM sections that define the intended operating environment of the product, at least at a high level. The purpose is to define the expected security functionality of the HDO environment (e.g., network firewall between device and external networks, DHCP service, NTP servers, creation of a private network segment, etc.). Reference the network diagram or other location in the SOM if the intended HDO environment is already depicted fully there.

# Network, Data Flow Diagram (DOC-10)

Add a comprehensive network and dataflow diagram to support the integration of the device in its intended operating environment.

* A Data Flow Diagram may comprise a depiction of data storage, data processors, any external interactions and the data flow between those instances. The diagram or its explanatory text should clearly label the various components and show the boundary that defines what is part of the product/system and what is an externally interfaced component.
* The Network Diagram typically comprises the device, its type of connectivity (e.g., DICOM) to HDO servers, firewalls and routers used and external connections. The elements in the diagram are supplemented by some verbal descriptions.

If the device interacts with PII in any way, two important requirements apply to the diagrams: (1) Data flow of PII through major components of the device must be clearly depicted, (2) a diagram must depict how the device will be embedded in a customer environment and clearly depict the application of privacy roles (e.g., GDPR-related role such as Data Controller or Data Processor and/or HIPAA-related role such as Business Associate).

**Note**: Example diagrams may be obtained from the various internal and external sources, such as the Mayo Clinic, whose vendor resources include an architecture diagram template.

# Setup of SaMD (DOC-11)

If the product is Software as a Medical Device (SaMD), provide the following specifications as they apply (Delete this section if the product is not SaMD):

* The operating system (OS) contained
* Any specifications which need to be considered if the owner/operator or customer is providing the operating system and needs to setup the SaMD properly
* Hosting details, including whether it is the customer or Stryker hosting the SaMD.

# MANAGEMENT OF PII and PHI (MPII-1)

If the device displays, transmits, stores, or modifies Personally Identifiable Information (PII, e.g., electronic Protected Health Information (ePHI)), provide a brief description of it.

Describe which privacy regulations were considered during the design and the development of the device (e.g., GDPR, HIPPA). In order to fill out the following sections completely check with the applicable privacy baseline requirements from D0000003422, Product security standard assessment.

If no PII is touched by the product, include a statement to that effect here, and then delete the subsections.

# Authority to Collect PHI

Describe any authority to collect PHI and all related legal agreements and consent decrees which have to be considered for the privacy compliant application of the device.

# Purpose Specification for PHI Use

Describe the official purpose for collection, transmission, or processing of personal data as outlined in the architectural document. Consider any purpose limitations. This should match what is listed in any official contracts or other documents for the product. Refer to baseline requirements for privacy in D0000003422, Product security standard assessment.

# PHI Data Quality and Integrity

Describe any mechanisms implemented in the device that will be used to keep data up to date, discover mistaken data, and correct data.

Provide instructions for any cases when customer involvement is needed to maintain data integrity.

Include a description (or reference to the AUDIT CONTROLS section) of which data processing functionality was established to ensure the integrity of the PII/PHI. For instance, an automatic audit function can be used to flag relevant changes to data.

# PHI Data Deletion and Minimization (SGUD-2)

Describe any functionality that allows data deletion to ensure that PII/PHI is not kept longer than defined in the purpose specification.

Describe which PII/PHI is marked with time stamp information to enable it to be selected for deletion on the basis of when it was acquired or stored.

Describe how the customer can follow applicable data minimization rules and explain how data may be deleted.

# Legal Roles and Related Requirements for Privacy

Describe if Stryker acts as a Data Controller and collects PHI, explaining the following:

* Describe any workflow which is set up (e.g., an electronic form or a notification) to ensure that a patient consent decree is required before any data processing starts.
* Describe how patients are informed about the data collection before any data processing starts.

Describe if Stryker is defined as Data Processor, explaining the following:

* Describe any applied warning statements (e.g. "This product processes personal data. The surgeon is responsible for obtaining patient consent for product use when appropriate.")

# Handling of Patient Requests for their PHI Access

Describe how the device supports requests of individuals for access to their Personal Information.

Describe how the device supports requests of individuals for deletion, restriction of processing, revision or portability of their Personal Information.

# Storage and Removal of PII (MPII-2)

If the device maintains personally identifiable information (PII) provide information/specifications concerning how PII is stored and PII is deleted, as applicable. Consider whether any of the following statements apply:

* PII is maintained temporarily in volatile memory (i.e., until cleared by power-off or reset)
* PII is persistently stored on internal media
* PII is preserved in the device’s non-volatile memory until explicitly erased, thus being maintained when the device is powered off and during power service interruptions
* PII is stored in a database
* Configuration allows to automatically delete local PII after it is stored to a long-term solution
* The process for manual or automatic PII deletion entails that the customer be informed so that the proper procedure is followed to ensure full deletion of the appropriate data.
* Data minimization or de-identification techniques are employed by the product (see section 9)
* Customer has access to settings that impact data minimization or de-identification and should be provided relevant instructions and warnings.

If any of the below capabilities apply, mention them here (because they relate to MDS2 questions in the MPII-2 family) but provide a more complete explanation in the next section (which applies more specifically to PII transfer issues).

* PII can be imported/exported with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)
* Internal media can be removed by a service technician (e.g., for separate destruction or customer retention)
* PII records can be stored in a separate location from the device’s operating system (i.e., secondary internal drive, alternate drive partition, or remote storage location)

# Transmitting, Importing/Exporting of PII (MPII-3)

If the device has mechanisms used for the transmitting, importing/exporting of PII specify them and consider hereby the following aspects:

* The display of PII (e.g., video display, etc.)
* Generation of hardcopy reports or images containing PII
* Retrieval of PII from or recording PII to removable media (e.g., removable-HDD, USB memory, DVD-R/RW, CD-R/RW, tape, CF/SD card, memory stick, etc.)
* PII is transmitted/received or imported/exported via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)
* PII is transmitted/received via a wired network connection (e.g., RJ45, fiber optic, etc.)
* PII is transmitted/received via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)
* PII is transmitted/received over an external network (e.g., Internet)
* PII is imported via scanning a document
* PII is transmitted/received via a proprietary protocol
* Any other mechanism used to transmit, import or export PII

# AUTOMATIC LOGOFF (ALOF-1, 2)

*The device's ability to prevent access and misuse by unauthorized users if the device is left idle for a period of time.*

If applicable, describe how the device can be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver). Also, if possible, describe how to setup the length of inactivity time before auto-logoff/screen.

# AUDIT CONTROLS (AUDT)

*The ability to reliably audit activity on the device.*

# Device-Specific Audit Log Configuration (AUDT-1)

If applicable, describe how device specific audit logs can be created. Also describe the type of PII which is recorded (e.g., user ID, other?).

# Events and Attributes Recorded (AUDT-2, 3, 4)

If events are recorded in the audit log indicate which of the following events are recorded in the audit log:

* Successful login/logout attempts
* Unsuccessful login/logout attempts
* Modification of user privileges
* Creation/modification/deletion of users
* Presentation of clinical data, PHI, and/or PII (e.g., display, print)
* Creation/modification/deletion of data
* Import/export of data from removable media (e.g., USB drive, external hard drive, DVD)
* Receipt/transmission of data or commands over a network or point-to-point connection
* Remote or on-site support
* Application Programming Interface (API) and similar activity
* Emergency access
* Marked personal data with time stamp information to enable it to be selected for deletion based on when it was acquired or stored
* Other events (e.g., software updates)

If the owner/operator can define or select which events are recorded in the audit log, describe which roles can perform configuration or management of the logs.

If data attributes can be captured in the audit log for an event, provide details.

If the audit log records date/time, describe if date and time can be synchronized by Network Time Protocol (NTP) or equivalent time source, and how to enable or manage the NTP time source.

# Audit Log Protection (AUDT-7)

Describe if audit logs are protected from modification.

Describe if audit logs are protected from access.

# Log Export, Use, and Notification (AUDT-5, 6, 8)

If audit log content can be exported, consider describing the following:

* Export via physical media
* Export via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM
* Export via other communications (e.g., external service device, mobile applications)
* Whether or not audit logs are encrypted in transit or on storage media

If audit logs can be monitored or reviewed by the owner/operator, describe how this can be done.

If the monitoring, review, or export of audit logs is limited to specific roles, explain.

Describe if audit logs can be analyzed by the device.

Describe whether the device provides notifications when it cannot write logs (e.g., if storage is full), and whether the device supports the presentation of alerts when specific conditions are met, such as suspicious activity recorded in a log or issues with log files.

Describe any relevant details related to audit logs that are not already covered above, such as log backup, retention, disposition, etc.

# AUTHORIZATION (AUTH)

The ability of the device to determine the authorization of users.

# Access Prevention (AUTH-1)

If the device allows for configurable access prevention to unauthorized users, describe how to setup any federated credentials management of users for authorization (e.g., LDAP, OAuth), including any group policy techniques (e.g., Active Directory) and/or any special groups, organizational units, or group policies required.

Also, add details if multi-factor authentication is employed or is available, how and when account locks occur, and if how password recovery is utilized, if applicable.

# Privilege and Access (AUTH-2, 3, 4, 5, SGUD-3, 3.1)

If users can be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)*, I*, identify the various roles and levels of access that are feasible within the system and provide the HDO IT department with enough information to select appropriate user roles to perform functional and security tasks. User roles may be very granular and customizable for some systems while other systems may only be capable of a limited number of user roles. For instance, a basic system may only support a device user role and a device administrator/maintainer role. Any pre-defined user roles should be listed along with their purpose and any special capabilities or access granted to the user roles

Describe how to setup those privilege levels, including any grant of unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account), as applicable. If applicable, describe the configuration mechanism for the device to authorize/control API access requests and/or operate in any restricted access mode or “kiosk mode.” Be sure the description clearly indicates whether the owner/operator can manage password control for all accounts. *If the device is integrated with enterprise or upstream identity and access management capability, describe that here.*

# System Use Notification

If the system is set to display a notification message or banner prior to granting access to the system, or if the customer has the capability to activate or configure such a notification, explain the details here.

*If the device is integrated with enterprise or upstream identity and access management capability, describe that here.*

# CYBER SECURITY PRODUCT UPGRADES (CSUP)

# Secure Servicing and Security Upgrades Overview (CSUP-1)

*The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.*

Briefly list and describe any software or firmware which may require security updates during its operational life, including the third-party software/firmware manufacturer. Point to applicable sections below for detailed information.

If security-related actions should be taken by the customer prior to any other kind of product servicing, explain the procedure here or point to the applicable sections where this is described. For example: “Sensitive/PII data must be removed from the device before product is serviced. Refer to data decommissioning instructions in section [number] below.”

# General Parameters for Updates (CSUP-7, 8, 9, 10, 11)

Consider and specify (when applicable) the following general instructions concerning updates/patches:

* Customer notifications when updates are approved for installation
* Automatic installation of software updates
* Approved list of third-party software that can be installed on the device
* Installation by owner/operator of manufacturer-approved third-party software
* Include any device mechanism to prevent installation of unapproved software
* Any information mechanism about review and approval status of updates
* Review cycle for the device

In connection with MDS2 question CSUP-11, this section should describe Stryker’s vulnerability assessment activities and/or refer to the vulnerability-related descriptions in Section 3.3, Related Manufacturer Programs.

# Operating System Updates (CSUP-2)

Specify the listed update/patch management elements if the device contains an OS which would require updates and/or patches:

* Instructions for the installation of patches or software updates (or ref.)
* Vendor-authorized service to install patches or software updates
* Remote installation of patches or software updates
* Security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer

# Driver, Firmware Updates (CSUP-3)

Specify the listed update/patch management elements if the device contains Drivers and Firmware which would require updates and/or patches:

* Instructions for the installation of patches or software updates (or ref.)
* Vendor-authorized service to install patches or software updates
* Remote installation of patches or software updates
* Security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer

# Anti-Malware Software Updates (CSUP-4)

Specify the listed update/patch management elements if the device contains Anti-Malware Software which would require updates and/or patches:

* Instructions for the installation of patches or software updates (or ref.)
* Vendor-authorized service to install patches or software updates
* Remote installation of patches or software updates
* Security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer

# COTS (non-OS) Updates (CSUP-5)

Specify the listed update/patch management mechanism for non-operating system commercial off-the-shelf software (COTS):

* Instructions for the installation of patches or software updates (or ref.)
* Vendor-authorized service to install patches or software updates
* Remote installation of patches or software updates
* Security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer

# Other Software Component Updates (CSUP-6)

Specify the listed update/patch management elements if the device contains other software components (e.g., asset management software, license management) which would require updates and/or patches then:

* Instructions for the installation of patches or software updates (or ref.)
* Vendor-authorized service to install patches or software updates
* Remote installation of patches or software updates
* Security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer

# HEALTH DATA DE-IDENTIFICATION (DIDT-1)

*The ability of the device to directly remove information that allows identification of a person.*

Describe any device capability to de-identify PII (e.g., automatic or manual anonymization, pseudonymization, etc.), or to de-anonymize PII (also reference D0000003422, Product security standard assessment, Privacy by Design Sub-element 2.7. Privacy Enhanced System Design and Development).

Describe any device de-identification profiles that comply with the DICOM standard for de-identification

# DATA BACKUP AND DISASTER RECOVERY (DTBK-1, 2, 3, 4, 5, 6)

The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.

Specify long term primary storage of PII/patient information

Specify any “factory reset” function to restore the original device settings

Describe the device backup capabilities considering:

* Integral data backup capability to removable media
* Backup capability to remote storage
* Backup capability for system configuration information, patch restoration, and software restoration
* Capability to check the integrity and authenticity of a backup

# EMERGENCY ACCESS (EMRG-1)

*The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.*

Describe any emergency access (i.e., “break-glass”) features.

# HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU-1, 2)

How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.

Describe any data integrity checking mechanisms of stored health data (e.g., hash or digital signature).

Describe any error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5). Refer to audit logs section, if applicable.

If customer involvement is required for the preservation of data integrity (especially for PII), describe the details here.

# MALWARE DETECTION/PROTECTION (MLDP-1)

*The ability of the device to effectively prevent, detect and remove malicious software (malware).*

Specify any executable software which can be hosted on the device.

# Support of Anti-Malware (MDLP-2)

Specify any features of anti-malware protection considering:

* Device includes anti-malware software by default
* Anti-malware software available as an option
* Owner/operator to install or update anti-malware software
* Owner/operator can independently (re-)configure anti-malware settings
* How notification of malware detection occurs in the device user interface
* Only Stryker authorized persons repair systems when malware has been detected
* Malware notifications written to a log
* Restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)

# Other Compensation/Protection Controls (MDLP-3, 4, 5)

If anti-malware cannot be installed on the device, specify any other compensating controls implemented, which may also include:

* Application whitelisting that restricts the software and services that are permitted to be run on the device
* Host-based intrusion detection/prevention system. Provide customer installation and configuration instruction, if there is any.

If customers are intended to be given access to perform security scans (e.g., vulnerability monitoring) on the device, explain the details, such as how to enable scanning and what tools can be configured to perform the scanning (example: running Nessus scans against the device).

# NODE AUTHENTICATION (NAUT-1, 2, 3)

*The ability of the device to authenticate communication partners/nodes.*

Describe any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g., Web APIs, SMTP, SNMP).

Describe any network access control mechanisms supported (e.g., does the device have an internal firewall, or use a network connection whitelist). Document firewall ruleset, if applicable.

Describe any certificate-based network connection authentication.

Describe any configuration details relevant to implementation of node authentication.

# CONNECTIVITY CAPABILITIES (CONN)

*All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.*

# Hardware Connectivity Capabilities (CONN-1)

Describe any hardware connectivity capabilities, especially considering:

* Wireless connections
* Wireless connections
  + WiFi (consider authentication protocols supported, such as WPA2 EAP-TLS)
  + Bluetooth (consider security modes supported)
  + Another wireless network connectivity (e.g., LTE, Zigbee, proprietary)
  + Other wireless connections (e.g., custom RF controls, wireless detectors)
* Physical connections
  + RJ45 Ethernet ports
  + USB ports
  + Removable memory devices
  + Other physical connectivity

Consider referencing authorization/authentication information elsewhere in this document, with a statement such as: “The security of the listed connections is enforced by security controls described above in section 7 (AUTH), section 14 (NAUT), and section 16 (PAUT).”

# Communication Provisions (CONN-2, 3, 4, 5, 6, 7)

Specify any other applicable communication provisions of the device, such as:

* List of network ports and protocols that are used or may be used on the device
* Communication with other systems within the customer environment
* Communication with other systems external to the customer environment (e.g., a service host)
* Ability to make or receive API calls
* Requirement of an internet connection for its intended use
* Whether or not the device supports Transport Layer Security (TLS), and if so, whether or not the TLS is configurable
* Operator control functionality from a separate device (e.g., telemedicine)

# PERSON AUTHENTICATION (PAUT)

*The ability to configure the device to authenticate users.*

# Password/ID Assignments (PAUT-1)

Provide information regarding the device behavior for password/ID enforcement: Does it support and enforce unique IDs and passwords for all users and roles (including service accounts)? What authentication mechanisms are supported/enforced for unique IDs, and are there any exceptions?

# User Account Management (PAUT-2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14)

Specify any supported person/user account/authentication management mechanism which applies from this list:

* Configuration to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)
* Configuration to lock out a user after a certain number of unsuccessful logon attempts
* All default accounts (e.g., technician service accounts, administrator accounts)
* How passwords can be changed
* Configuration to enforce creation of user account passwords that meet established (organization specific) complexity rules
* Support of any account passwords that expire periodically
* Support of multi-factor authentication
* Support of single sign-on (SSO)
* How to disable/lock on the device
* Support of biometric controls
* Support of physical tokens (e.g., badge access)
* Support of group authentication (e.g., hospital teams)
* Storage/management of authentication credentials, including use of secure storage method

# PHYSICAL LOCKS (PLOK-1, 2, 3)

*Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media.*

If the device is NOT software only, specify any applicable physical locking mechanism:

* Are all device components maintaining PII (other than removable media) physically secure (i.e., cannot be removed without tools)?
* Are all device components maintaining PII (other than removable media) physically secured behind an individually keyed locking device?
* Does the device have an option for the customer to attach a physical lock to restrict access to removable media?

# ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

*Manufacturer’s plans for security support of third-party components within the device’s life cycle.*

Describe any secure software development processes or standards following during product development, such as ISO/IEC 27034 or IEC 62304.

Include a description of how Stryker evaluated third-party applications and software components included in the device for secure development practices, if applicable.

If applicable, provide the customer-facing web page or other source of information on software support dates and updates.

Explain if Stryker has a plan for managing third-party component end-of-life.

# SOFTWARE BILL OF MATERIALS (SBoM-1, 3)

*This section supports controls in the RDMP section.*

Include the Software Bill of Materials in an appendix, attachment, or referenced external location where the SBoM may be obtained. If a list of the installed software components on the device can be generated describe the command or process method which creates this list.

# SBoM Structure and Updates (SBoM-2, 4)

Explain what standard or nonstandard method the SBoM follows in describing software components, including details such as the following:

* Are the developers/manufacturers of the software components identified?
* Are the major version numbers of the software components identified?
* Are any additional descriptive elements identified?

If there is an update process for the SBoM, explain.

# SYSTEM AND APPLICATION HARDENING (SAHD)

*The device's inherent resistance to cyber-attacks and malware.*

Explain whether the device is hardened in accordance with any industry standards, and whether it has received any cybersecurity certifications.

Explain system and application hardening details that apply, considering the questions below:

* Does the device employ any mechanisms for software integrity checking?
* Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?
* Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?
* Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?
* Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?
* Does the device provide role-based access controls?
* Are any system or user accounts restricted or disabled by the manufacturer at system delivery?
* Are any system or user accounts configurable by the end user after initial configuration?
* Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?
* Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?
* Are all communication ports and protocols that are not required for the intended use of the device disabled?
* Are all services (e.g., telnet, file transfer protocol (FTP), internet information server (IIS), etc.), which are not required for the intended use of the device deleted/disabled?
* Are all applications (COTS applications as well as OS-included applications, e.g., Microsoft Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?
* Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?
* Can unauthorized software or hardware be installed on the device without the use of physical tools?
* Are other endpoint protections employed?
* Does the product documentation include information on operational network security scanning by users?
* Can the device be hardened beyond the default provided state?
* Are instructions available from vendor for increased hardening?
* Can the system prevent access to BIOS or other bootloaders during boot?
* Have additional hardening methods been used?

# HEALTH DATA STORAGE CONFIDENTIALITY (STCF-1, 2, 3, 4)

*The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.*

If data at rest is encrypted specify the following (as it applies):

* PII which is encrypted and PII which is not encrypted
  + Encryption method used
  + Customer instruction to configure encryption
* Change or configuration instruction of encryption keys
* Data storage place: database located on the device or in a database external to the device

For additional context and requirements, refer to D0000003422, Product security standard assessment, Privacy by Design Sub-element 2.7. Privacy Enhanced System Design and Development.

# TRANSMISSION CONFIDENTIALITY (TXCF)

*The ability of the device to ensure the confidentiality of transmitted personally identifiable information.*

Specify how the device ensures confidentiality of PII or data in general:

* Can personally identifiable information be transmitted only via a point-to-point dedicated cable?
* Is personally identifiable information encrypted prior to transmission via a network or removable media?
* If data is not encrypted by default, can the customer configure encryption options?
* Is personally identifiable information transmission restricted to a fixed list of network destinations?
* Are connections limited to authenticated systems?
* Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?

For additional context and requirements, refer to D0000003422, Product security standard assessment, Privacy by Design Sub-element 2.7. Privacy Enhanced System Design and Development.

# TRANSMISSION INTEGRITY (TXIG-1, 2)

*The ability of the device to ensure the integrity of transmitted data.*

Specify any applied mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission.

If the device includes multiple sub-components connected by external cables, specify them here (or provide a ref. to the according specification).

# REMOTE SERVICE (RMOT-1, 2, 3)

*Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.*

If the device offers remote service connections for device analysis or repair, provide related instructions and information, considering the following:

* Owner/operator initiation of remote service sessions for device analysis or repair
* Indication of an enabled and active remote session
* Patient data that will be accessed or viewed from the device during the remote session

If the device permits or uses remote service connections for predictive maintenance data, specify the connections.

If the device has any other remotely accessible functionality (e.g., software updates, remote training), provide specifics.

# SECURITY PROGRAM INTEGRATION

Complete this section and its subsections to provide an overview of secure integration activities. Some content is prepopulated but may be edited to conform with the specific circumstances of the product and the SOM. If the product is SaMD, some integration information will already be present in the section related to question DOC-11, and the present section can refer to the prior section as appropriate.

This section provides configuration guidance to enable the customer to achieve compliance when integrating the product.

# Vulnerability Management

Section 3.3, Related Manufacturer Programs, defines Stryker’s process for vulnerability identification, assessment, and communication. See Section 8, CYBER SECURITY PRODUCT UPGRADES, for information regarding software patches.

# Incident Response

The content of this section should include granular incident response actions that can be taken by the HDO IT department and should be based on the product risk assessment. The content should answer the question: If a risk is realized, what do I, as the HDO IT department, do about it? This should be answered for at least all major types of cybersecurity risks, but for most systems it will be possible to summarize HDO IT departmental responses or actions. For embedded type systems and those with restricted user interfaces, a set of acceptable HDO IT department incident response actions combined with leveraging Stryker maintenance capabilities may be required. At a minimum, a set of procedures appropriate to the system should be developed and provided to address the following categories of incidents as they may apply to the system:

* Suspected malware on the system
* Confirmed malware on the system
* Unexpected system behavior
* Recovery of data from a damaged or non-functional system
* Suspected misuse of the device (how to confirm through logs)
* Methods to determine if data was inappropriately accessed or copied from the device
* Forensic inspection of the device

# Security Testing

As appropriate, provide specific or special procedures required to test or validate the effectiveness of system security function. The purpose is to assist the HDO IT department to meet departmental requirements related to compliance frameworks. Only items that require unique or specialized procedures should be documented here. If the device software is limited to software on a standard Operating System, this section may explain, “The product is installed on a general-purpose operating system, and Stryker has evaluated that standard security testing methodologies commonly employed for the Operating System type are appropriate. No special procedures for security testing are required beyond those typically applied to the Operating System.”

# Scanning

If any physical network interfaces exist on the device, provide information necessary to conduct scanning or manual vulnerability analysis of the system, as appropriate. Refer to section 13.2, Other Compensation/Protection Controls, as appropriate for additional details related to scanning configuration.

# Risk Management

Stryker integrates cyber security risk management into its overall program for health and safety risk management. Both security and safety risk assessment were conducted for this device per guidelines in AAMI TIR57 and in compliance with EN/ISO 14971. Additionally, Stryker has a robust post market security risk management process which monitors the ongoing security posture of this device and addresses any security incidents that might arise.

# Training and Awareness

Identify any special training or awareness that may be required. If nothing specific to the system is required, insert text similar to the following: “Stryker has evaluated the security training requirements for this product and determined that standard user security and awareness training commonly provided to users of general-purpose business computing environments is sufficient for standard users. System administrators or security administrators should review this manual to familiarize themselves with the security relevant functionality of the system.”

# SECURE DECOMMISSIONING

Include specific instructions to decommission or dispose of system components (assets). Also, explain recommended or required actions related to the handling of data during decommissioning, such as:

* What steps to take to delete data or make it inaccessible through key destruction
* What happens to data when the product is reinitialized
* How to security decommission data when the product is non-functional
* Whether decommissioning can happen locally or remotely
* Whether and how to remove sensitive data before product is serviced

**Note:** A **REVISION HISTORY** section may be added if the revision history details are expected to be relevant for the customer, such as to highlight the sections that have been updated to account for new features or controls.