‘’

Smart Medic Device

Security Operations Manual

Stryker

Prepared by: G’ SECURE LABS

Disclaimer: The recommendations contained in this report are based on industry standard “Best Practices”. Best practices are, by necessity, generic in nature and may not take into account exacerbating or mitigating circumstances. These recommendations, even if correctly applied, may cause conflicts in the operating system or installed applications. Any recommended changes to the operating system or installed application should first be evaluated in a non-production environment before being deployed in the production environment.

**G’ Secure Labs**

Recipient:

|  |  |
| --- | --- |
| Name/role | Company |
| Deepak | Stryker |

Document Version:

|  |  |  |  |
| --- | --- | --- | --- |
| Name of the Author | Version | Title | Date |
| GSL Team | 1.0 | Security Operations Manual | 21/10/2021 |

Table of Contents

[1. Purpose 6](#_Toc86061142)

[2. Definition 6](#_Toc86061143)

[3. Automatic Logoff 8](#_Toc86061144)

[4. Audit Controls 8](#_Toc86061145)

[4.1 Device-Specific Audit Log Configuration 8](#_Toc86061146)

[4.2 Events and Attributes Recorded 8](#_Toc86061147)

[4.3 Audit Log Protection 9](#_Toc86061148)

[4.4 Log Export, Use, and Notification 10](#_Toc86061149)

[5. Authorization 10](#_Toc86061150)

[5.1 Access Prevention 10](#_Toc86061151)

[5.2 Privilege and Access 10](#_Toc86061152)

[5.3 System Use Notification 11](#_Toc86061153)

[6. Cyber Security Product Upgrades 11](#_Toc86061154)

[6.1 Secure Servicing and Security Upgrades Overview 11](#_Toc86061155)

[6.2 General Parameters for Updates 11](#_Toc86061156)

[6.3 Operating System Updates 12](#_Toc86061157)

[6.4 Driver, Firmware Updates 12](#_Toc86061158)

[6.5 Anti-Malware Software Updates 13](#_Toc86061159)

[6.6 COTS (non-OS) Updates 13](#_Toc86061160)

[6.7 Other Software Component Updates 14](#_Toc86061161)

[6.8 Data Backup and Disaster Recovery 14](#_Toc86061162)

[7. Emergency Access 16](#_Toc86061164)

[8. Health Data Integrity and Authenticity 16](#_Toc86061165)

[9. Malware Detection/Protection 16](#_Toc86061166)

[9.1 Support of Anti-Malware 17](#_Toc86061167)

[9.2 Other Compensation/Protection Controls 17](#_Toc86061168)

[10. Node Authentication 18](#_Toc86061169)

[11. Connectivity Capabilities 18](#_Toc86061170)

[11.1 Hardware Connectivity Capabilities 18](#_Toc86061171)

[11.2 Communication Provisions 19](#_Toc86061172)

[12. Person Authentication 20](#_Toc86061173)

[12.1 Password/ID Assignments 20](#_Toc86061174)

[12.2 User Account Management 20](#_Toc86061175)

[13. Physical Locks 21](#_Toc86061176)

[14. Roadmap for Third Party Components in Device Life Cycle 22](#_Toc86061177)

[15. System and Application Hardening 22](#_Toc86061178)

[16. Health Data Storage Confidentiality 25](#_Toc86061179)

[17. Transmission Confidentiality 25](#_Toc86061180)

[18. Transmission Integrity 26](#_Toc86061181)

[19. Remote Service 26](#_Toc86061182)

[20. Security Program Integration 26](#_Toc86061183)

[21. Secure Decommissioning 27](#_Toc86061184)

1. **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.

1. **Definition**

* **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.
* **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.
* **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.
* **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.
* **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.
* **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.
* **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.

# Automatic Logoff

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

* Device should automatically logoff when Idle
* Device active session should get automatically locked when Idle
* Device should be password protected when Idle
* Device screen saver should get activated when Idle
* Customer should setup the length of inactivity time before auto-logoff/screen

# Audit Controls

The ability to reliably audit activity on the device.

# Device-Specific Audit Log Configuration

Audit control should be implemented and adopted by the hospital.

* Data Backup and recovery
* Data Recovery and Role swap
* Inventory management
* IT policy controls
* Mobile device/application management
* All the Audit Control and evidences should be well maintained.
* Periodic audit should be performed for the devices used within hospital
* Client should maintain audit log of users who are accessing device from remote location

# Events and Attributes Recorded

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

**Successful login/logout attempts**

* Authorized uses should have access to the device
* Role based access controls should be provided to each users accessing the device ex: HR, Admin, Users
* Elevated privileged users should have full access to the device such as Read, write and execute
* Unprivileged users access to the device should have Read Access

**Unsuccessful login/logout attempts**

* Login attempts should be limited by three
* Account should have a captcha login
* After 3 attempts on unsuccessful login the device should have reset control in place

**Modification of user privileges**

* Horizontal and Vertical privileged user’s modification should be logged
* Business Approval should be taken before any changes made in the system

**Creation/modification/deletion of users**

* Logs should be maintained for all the activities on devices
* Monitoring – To detect unusual activity, reporting alerts and event in real-time

**Creation/modification/deletion of data**

* Logs should be maintained for all the activities on device
* Monitoring – To detect unusual activity, reporting alerts and event in real-time

**Remote or on-site support**

* On-site and off-site support should be available for customers by raising the ticket/customers care help line

**Application Programming Interface (API) and similar activity**

* API would be used to transmit the data in transit
* Data from the API call would be stored in Database
* Assurance on accuracy of data should be maintain by implementing the encryption mechanism

**Emergency access (Break-Glass Control should be implemented)**

* In case of emergency access, the Break glass control should be applied
* Marked personal data with time stamp information to enable it to be selected for deletion based on when it was acquired or stored
* Data should be discarded after 6 months from the date of generation
* Other events (e.g., software updates)
* Patching should be applied as soon as the patches are released

**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.**

* Recording of logs both locally and to a remote log server

**Data attributes can be captured in the audit log for an event, provide details.**

* To check with the client on the scope of audit log capture

**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.**

* Yes, audit log should record Date/Time and it should be synchronized with NTP, for keeping the track record. Setting of NTP depends on the which Operating systems is been used.

# Audit Log Protection

**Audit logs are protected from modification.**

* Encrypt the data at rest – (When the data is stored in the devices)

**Audit logs are protected from access.**

* Password protection to devices login
* Authorized users are providing the access to the data

# Log Export, Use, and Notification

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

**Whether audit logs are encrypted in transit or on storage media**

* Encrypt logs in the storage system to protect data when they are taken out of it.
* Audit logs can be monitored or reviewed by the owner/operator, how this can be done. If the monitoring, review, or export of audit logs is limited to specific roles.
* 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.

# Authorization

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

# Access Prevention

**The device allows for configurable access prevention to unauthorized users, describe how to setup any federated credentials management of users for authorization.**

* Client can also provide review accesses to confirm only those who require access to device.

**Multi-factor authentication is employed or is available, how and when account locks occur, and if how password recovery is utilized. With OTPs a new code is generated periodically or each time an authentication request is submitted.**

* Authenticator Application can generate new code periodically or each time an authentication request is submitted.
* To unlock your account, you will be required to either answer 3 of your security questions, or correctly enter information about your account. To unlock your account, you will be required to either answer 3 of your security questions, or correctly enter information about your account.

# Privilege and Access

**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**

* Only assigning privileged roles/accounts to staff who have an appropriate security clearance.
* Only granting privileged system accesses on a temporary or as-needed basis.
* Regularly reviewing accesses to privileged roles and accounts.
* Increasing monitoring of staff with privileged system access such as ‘admin’ access.
* Audit logging and regularly reporting the use of privileged accounts.
* Confirm that someone cannot bypass standard process requirements even when subject to pressure.
* Confirm that privileged accounts are subject to separation of duties requirements.

**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. The configuration mechanism for the device to authorize/control API access requests and/or operate in any restricted access mode or “kiosk mode.”**

* Maintain an up-to-date inventory of all privileged accounts
* Do not allow admins to share accounts.
* Minimize the number of privileged accounts.
* Create a password policy and strictly enforce it.
* Require multifactor authentication for privileged accounts If the device is integrated with enterprise or upstream identity and access management capability, describe that here.

# System Use Notification

* Client has to turn off all the visibility of notification if the system is in lock and log off mode.If the device is integrated with enterprise or upstream identity and access management capability, describe that here.

# Cyber Security Product Upgrades

# Secure Servicing and Security Upgrades Overview

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.**

* The ability of on-site service staff, remote service staff to install or upgrade
* Client need to patches device's security.
* Authorized customer or staff need to install/upgrade software or hardware or firmware.
* Customer need to update the third-party software or firmware if needed.

**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:**

# General Parameters for Updates

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

**Customer notifications when updates are approved for installation**

* When updates are approved customer should get notification.

**Automatic installation of software updates**

* Customer can be provided automatic installation of software updates

**Approved list of third-party software that can be installed on the device**

* Approved list of third-party software that can be installed on the device

**Installation by owner/operator of manufacturer-approved third-party software**

* Owner/operator of manufacturer-approved third-party software should be install on device.

**Include any device mechanism to prevent installation of unapproved software**

* Include only approved software to prevent the device.

# Operating System Updates

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.)**

* Customer can be provided automatic installation of software updates
* Authorized customer or staff need to install/upgrade software or hardware.Authorized customer or staff need to install/upgrade software or hardware or firmware.Authorized customer or staff need to install/upgrade software or hardware or firmware.Authorized customer or staff need to install/upgrade software or hardware or firmware.Authorized customer or staff need to install/upgrade software or hardware or firmware.Authorized customer or staff need to install/upgrade software or hardware or firmware.Authorized customer or staff need to install/upgrade software or hardware or firmware.

**Remote installation of patches or software updates**

* There should be remote installation for patches or software updates as per customer requirement.
* On-site and off-site support should be available for customers by raising the ticket/customers care help line.

**Security updates from any third-party manufacturers to be installed without approval from the manufacturer**

* Approved list of third-party software that can be installed on the device
* Installation by owner/operator of manufacturer-approved third-party software

# Driver, Firmware Updates

**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.)
* Customer can be provided automatic installation of software updates
* Authorized customer or staff need to install/upgrade software or hardware or firmware

**Remote installation of patches or software updates**

* On-site and off-site support should be available for customers by raising the ticket/customers care help line.

**Security updates from any third-party manufacturers to be installed without approval from the manufacturer**

* Approved list of third-party software that can be installed on the device
* Installation by owner/operator of manufacturer-approved third-party software

# Anti-Malware Software Updates

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.)**

* Customer can be provided automatic installation of software updates
* Authorized customer or staff need to install/upgrade software or hardware

**Remote installation of patches or software updates**

* On-site and off-site support should be available for customers by raising the ticket/customers care help line.

**Security updates from any third-party manufacturers to be installed without approval from the manufacturer**

* Approved list of third-party software that can be installed on the device
* Installation by owner/operator of manufacturer-approved third-party software

# COTS (non-OS) Updates

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.)**

* Customer can be provided automatic installation of software updates
* Authorized customer or staff need to install/upgrade software or hardware

**Remote installation of patches or software updates**

* On-site and off-site support should be available for customers by raising the ticket/customers care help line.

**Security updates from any third-party manufacturers to be installed without approval from the manufacturer**

* Approved list of third-party software that can be installed on the device
* Installation by owner/operator of manufacturer-approved third-party software

# Other Software Component Updates

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.)**

* Customer can be provided automatic installation of software updates
* Authorized customer or staff need to install/upgrade software or hardware

**Remote installation of patches or software updates**

* On-site and off-site support should be available for customers by raising the ticket/customers care help line.

**Security updates from any third-party manufacturers to be installed without approval from the manufacturer**

* Approved list of third-party software that can be installed on the device
* Installation by owner/operator of manufacturer-approved third-party software

# Data Backup and Disaster Recovery

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

**HIPAA compliance and security**

The HIPAA Security Rule covers measures that restrict unauthorized access to sensitive data. Covered entities must defend against threats to sensitive data that can be reasonably anticipated. It also requires technical, administrative and physical safeguards to protect sensitive data.

What follows are examples of these three safeguards:

* **Technical safeguards** cover the use of firewalls, [encryption](https://searchsecurity.techtarget.com/definition/encryption) and other technology.
* **Physical safeguards** include locking up physical records and electronic devices containing PHI.
* **Administrative safeguards** may include policies that limit PHI access to certain people, safety awareness training and other people-based approaches to security.
  + Covered entities must evaluate IT capabilities and the likelihood of a PHI security risk. The HIPAA rules does not specify the types of technology to be used, but it should include [actions to keep hackers](https://www.computerweekly.com/feature/How-can-healthcare-organisations-fight-increased-cyber-crime-in-2021) and [malware](https://searchsecurity.techtarget.com/definition/malware) from gaining access to patient data.

The Health Insurance Portability and Accountability Act ([HIPAA](https://searchhealthit.techtarget.com/definition/HIPAA)) of 1996 is the primary law that oversees the use of, access to and disclosure of PHI in the United States. HIPAA defines PHI as data that relates to the past, present or future health of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual. HIPAA regulates how this data is created, collected, transmitted, maintained and stored by any HIPAA-covered organization. The Health Insurance Portability and Accountability Act ([HIPAA](https://searchhealthit.techtarget.com/definition/HIPAA)) of 1996 is the primary law that oversees the use of, access to and disclosure of PHI in the United States. HIPAA defines PHI as data that relates to the past, present or future health of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual. HIPAA regulates how this data is created, collected, transmitted, maintained and stored by any HIPAA-covered organization.

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

Describe the device backup capabilities considering:

**Integral data backup capability to removable media**

* There are three types of Backup Incremental, Full and Partial. Business and the service owners need to decide what kind of back up need to be taken.
* While backup the data - Recovery Time object (RTO) and Recovery Point Object (RPO) should be considered
* Removable media appliances often include storage, which comes as a 19” rack-mounted device that you install and connect to your network. The appliances are easy to install and configure. In most cases, you do not need to provision a separate server, operating system, or install any software. The agents installed on your systems perform the backups, and you access the solution via a graphical interface provided with the appliance.
* If you have enough capacity on your local disks, you can back up to them or to external USB drives. These backups are fast and convenient and you don’t need a network. The downside of local backups is that if the system is destroyed by fire of flood, your backups can be destroyed as well if they are stored in the same location. Also in many cases, you need to manage these backups on a computer-by-computer basis, which makes it cumbersome for larger environments.
* Local and USB disk backups are best for quick backups of a small number of systems and are designed for the recovery of individual files or systems in the event of software failure.
* However, remember that if you have a hardware appliance and it fails, you lose your entire data backup solution. Even if you backed up to a secondary location, you need to re-provision the backup solution before you can recover, which increases your recovery times.

**Backup capability to remote storage**

* The modern alternative to tape backup is cloud storage. With this type of solution, you subscribe to a certain storage capacity in the cloud operator’s or service provider’s data center. You do not need any hardware as you do with tape drives, but you do need an internet connection to send backups to the cloud
* In many cases, you can install the software on a virtual machine (VM). In many cases, you can install the software on a virtual machine (VM). In many cases, you can install the software on a virtual machine (VM). In many cases, you can install the software on a virtual machine (VM). In many cases, you can install the software on a virtual machine (VM). The modern alternative to tape backup is [cloud storage](https://www.acronis.com/en-us/cloud/storage/). With this type of solution, you subscribe to a certain storage capacity in the cloud vendor’s or service provider’s data center. You do not need any hardware as you do with tape drives, but you do need an internet connection to send backups to the cloud. Your vendor may have ways to eliminate the problems with uploading large amounts of data by offering physical data shipping or initial seeding program. To select the right solution, you need to develop a storage strategy based on your unique business requirements, RPOs, and RTOs. You also need a data backup solution that follows the industry-accepted 3-2-1 backup approach — store your data in three places, on two types of storage, with one copy stored off-site. Great examples of the 3-2-1 strategy are disk-to-disk-to-tape (D2D2T) and disk-to-disk-to-cloud (D2D2C) solutions. With these solutions, you back up your data to your central network storage and then copy that same backup to tape or off-site cloud storage. To select the right solution, you need to develop a storage strategy based on your unique business requirements, RPOs, and RTOs. You also need a data backup solution that follows the industry-accepted 3-2-1 backup approach — store your data in three places, on two types of storage, with one copy stored off-site. Great examples of the 3-2-1 strategy are disk-to-disk-to-tape (D2D2T) and disk-to-disk-to-cloud (D2D2C) solutions. With these solutions, you back up your data to your central network storage and then copy that same backup to tape or off-site cloud storage.

**Backup capability for system configuration information, patch restoration, and software restoration**

* [To create a backup](https://docs.bmc.com/docs/ars1805/backing-up-and-restoring-centralized-configuration-settings-804713498.html#Backingupandrestoringcentralizedconfigurationsettings-Tocreateabackup)
* [To restore a selected backup](https://docs.bmc.com/docs/ars1805/backing-up-and-restoring-centralized-configuration-settings-804713498.html#Backingupandrestoringcentralizedconfigurationsettings-Torestoreaselectedbackup)
* [To delete a selected backup](https://docs.bmc.com/docs/ars1805/backing-up-and-restoring-centralized-configuration-settings-804713498.html#Backingupandrestoringcentralizedconfigurationsettings-Todeleteaselectedbackup)
* Capability to check the integrity and authenticity of a backup
* Corruption Testing Corruption Testing Corruption Testing

# *Secure Storage Secure Storage*

* Backup Capability
* Virtual Infrastructure
* Logging

# Emergency Access

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.

**Any emergency access (i.e., “break-glass”) features.**

* The system administrator should document any actual emergency access for later audit & review
* A special audit trail is created to monitor such access. Standard access controls should be established with sufficient rules to minimize the number of times break–the–glass needs to occur.
* Break–glass is based upon pre–staged “emergency” user accounts, managed in a way that can make them available with reasonable administrative overhead.
* This solution can be used with a broad range of existing systems and architectures that require operators to login, such as with username and password, before access is granted.
* The break–glass intended to specifically cover emergency cases and should not be used as a replacement for a helpdesk.

# Health Data Integrity and Authenticity

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.

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

* Hashing algorithm should be implemented
* RSA algorithm should be implemented.

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

* Backups are often the only way to recover lost data from a power outage

# Malware Detection/Protection

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

Specify any features of anti-malware protection considering:

**Device includes anti-malware software by default**

* Anti-malware software should be provided by default prevent, detect and remove malware to prevent, detect and remove malware.

**Anti-malware software available as an option**

* Bitdefender Mobile Security & Antivirus
* Lookout Mobile Security Antivirus & Security
* ESET Mobile Security & Antivirus
* Trend Micro
* Malwarebytes Security
* Comodo Mobile Security

**Owner/operator to install or update anti-malware software**

* Yes U’’Owner/Operator need to install anti-malware software and Update too.

**Owner/operator can independently (re-)configure anti-malware settings**

* Install Anti-virus software.
* Regularly update software.
* Need to install Firewall.
* Client to patch or update the software, if needed.

**Third-party manufacturers need to upgrade the software and firmware.**

* Client have to patch or update the software, if needed.

**How notification of malware detection occurs in the device user interface**

* it can display a notification message to inform the user about the detection.  It can display a notification message to inform the user about the detection.

**Only Stryker authorized persons repair systems when malware has been detected.**

* Only authorized incident response team in the organization shall investigate and mitigate virus.

# Other Compensation/Protection Controls

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

**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).**

* Nessus can be considered the other network scanning tool used to ensure the security of the application by magnifying the vulnerabilities.

**Enable or Disable a Scanner for Nessus**

* In the top navigation bar, click Sensors. The Linked Agents page appears. ...
* In the left navigation bar, click Linked Scanners.
* In the scanners table, in the row for the scanner that you want to enable, hover over the button, which becomes.
* Click the button. The scanner is enabled

# Node Authentication

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

**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).**

* Authenticate using password such as Auth0

**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.**

* There should be internal firewall.

**Any certificate-based network connection authentication.**

* Digital Certificate and SSL certificate to be enabled.

# Connectivity Capabilities

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

Describe any hardware connectivity capabilities, especially considering:

* Wireless connections

**Wireless connections**

* Wi-Fi (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

# Communication Provisions

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**

* To check with Operator what port will be open to on public platform

**Communication with other systems within the customer environment**

* TLS 1.2 or higher should be implemented

**Communication with other systems external to the customer environment (e.g., a service host)**

* TLS 1.2 or higher should be implemented

**Ability to make or receive API calls**

* TLS 1.2 or higher should be implemented **Authentication** – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives. **Authentication** – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives. **Authentication** – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives. **Authentication** – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives. **Authentication** – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives.
* Authentication – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives.

**Requirement of an internet connection for its intended use**

* Customer need to have good internet connection to Login.

**Whether or not the device supports Transport Layer Security (TLS), and if so, whether or not the TLS is configurable Authentication – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives.**

**Operator control functionality from a separate device (e.g., telemedicine)**

* Authentication – Determining the identity of an end user. In a REST API, basic authentication can be implemented using the TLS protocol, but OAuth 2 and OpenID Connect are more secure alternatives.

# Person Authentication

The ability to configure the device to authenticate users.

# Password/ID Assignments

**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?**

* Limiting the number of attempts that a password can be tried.
* Introducing time delays between successive attempts.
* Locking accounts out after unsuccessful logon attempts.
* Enable security auditing to help monitor and track password attack.
* Implement password policies like using punctuation characters, upper and lowercase letters, special characters and numbers.

# User Account Management

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.)**

* Domain controller should be implemented within the organization
* All the devices and users should be configuring in Domain controller tool

**Configuration to lock out a user after a certain number of unsuccessful logon attempts**

* Account should be locked out after 3 attempts
* Captcha mechanism should be enabled, to avoid automated attacks

**All default accounts (e.g., technician service accounts, administrator accounts)**

* Default accounts – Username and password should be changed

**How passwords can be changed**

* OTP code to change the password.
* Secret questions to change the password.
* Using 2FA authenticator application.

**Support of any account passwords that expire periodically**

* Password changes should be auto enable after 30 days

**Support of multi-factor authentication**

* 2FA can be enabled to get the code via Voice, message or 2FA authenticator application.

**Support of single sign-on (SSO)**

* SAML authentication can be implemented.

**How to disable/lock on the device**

* Auto locks can be used by setting a timer.
* Manual locking mechanism can also be activated.

**Support of biometric controls**

* Biometric controls can be implemented to support login such as Faces scanning, finger print scanning etc.

**Support of physical tokens (e.g., badge access**

* RSA key token systems can be implemented for login validation.

**Support of group authentication (e.g., hospital teams)**

* Roles based access controls should be implemented
* This would provide access to authorized users only

**Storage/management of authentication credentials, including use of secure storage method**

* Credential should be stored in with data
* Encryption mechanism should be implemented

# Physical Locks

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:**

* All device components maintain sensitive data (other than removable media) physically secure (i.e., cannot be removed without tools)?
* All device components maintain sensitive data (other than removable media) physically secured behind an individually keyed locking device?
* The device has 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

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

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

* If client need to secure any software development process or standard during product development such 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.**

# System and Application Hardening

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?**

* Software updates and patching should be done from a reliable source

**Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?**

* Any software deployments should be testing prior and implemented

**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?**

* Software updates and patching should be done from a reliable and trusted source
* Organization should subscribe to the automatics patching before released in markets

**Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?**

* Monitoring tools can provide alerts and generate events
* Establishing an intrusion prevention system (IPS) or intrusion detection system (IDS)

**Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?**

* Access controls policies should be implements to restricts unauthorized access.

**Does the device provide role-based access controls?**

* Yes, role based access controls should be implemented

**Are any system or user accounts restricted or disabled by the manufacturer at system delivery?**

* Check with operator

**Are any system or user accounts configurable by the end user after initial configuration?**

* Yes, Once the systems are configured. Users can login to the devices.

**Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?**

* Yes, initially least privileged access should be granted. Then users can raise additional access request as per the need.

**Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?**

* Client need to check whether all services like telnet, File transfer protocol(FTP), internet information server(IIS) which are needed on device or which need to disabled on device.
* Block any unused or unneeded open network ports
* Disable and remove unnecessary protocols and services

**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?**

* Block any unused or unneeded open network ports
* Disable and remove unnecessary protocols and services

**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?**

* Restrict access to applications based on user roles and context (such as with application control)

**Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?**

* External media access should be restricted or blocked

**Can unauthorized software or hardware be installed on the device without the use of physical tools?**

* Unauthorized software and hardware should be disable and dealt with system administrator permissions.

**Are other endpoint protections employed?**

* Regularly updating third-party software essential to the operation of the server and removing third-party software that doesn’t conform to established cybersecurity standards
* Ensure your firewall is properly configured and that all rules are regularly audited
* Using antivirus, malware, and spyware protection applications

**Does the product documentation include information on operational network security scanning by users?**

* No, the product documentation should not include Operation Network Security scanning to users due to confidentiality purpose

**Can the device be hardened beyond the default provided state?**

* Yes, Devices is always Hardened beyond the default state

**Can the system prevent access to BIOS or other bootloaders during boot?**

* Enabling and configuring [Secure Boot](https://www.trentonsystems.com/blog/what-is-secure-boot)
* Restrict access to Boot

**Have additional hardening methods been used?**

* Ensure your firewall is properly configured and that all rules are regularly audited
* Using antivirus, malware, and spyware protection applications
* Using software-based data encryption
* Password policies as implemented
* Enabling and configuring [Secure Boot](https://www.trentonsystems.com/blog/what-is-secure-boot)
* Limiting and authenticating system access permissions
* Limiting or eliminating the creation and logging in of user accounts
* Client need to check whether all services like telnet, File transfer protocol(FTP), internet information server(IIS) which are needed on device or which need to disabled on device.
* Block any unused or unneeded open network ports
* Disable and remove unnecessary protocols and services.
* Restrict access to applications based on user roles and context (such as with application control)
* Application passwords should then be managed via an application password management/privileged password management solution, that enforces password best practices (password rotation, length, etc.)
* Implement privileged user controls
* Encrypt local storage
* There should be registry and other systems permissions to be enabled on device
* Encrypt network traffic if needed
* Remove unnecessary drivers, file sharing, libraries, software, services, and functionality
* Secure remote access points and users
* Restricting administrators and administrative privileges and functions
* Encrypting in-transit and at-rest database information (Disable caching for user responses that contain sensitive data, never store sensitive data that is no longer needed, encrypt all sensitive information that does need to be stored)

# Health Data Storage Confidentiality

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):**

* Disable caching for user responses that contain sensitive data
* Never store sensitive data that is no longer needed
* Encrypt all sensitive information that does need to be stored

**Sensitive data which is encrypted and Sensitive data 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**

* Any data stored on a medical device should be encrypted, if possible Any data stored on a medical device should be encrypted, if possible

# Transmission Confidentiality

The ability of the device to ensure the confidentiality of transmitted Sensitive data.

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

**Can sensitive data be transmitted only via a point-to-point dedicated medium?**

* Any data transmitted by the device should utilize approved secure transmission protocols (MQTT)
* Transmission of data should not be limited to point-to-point cables

**Is sensitive data encrypted prior to transmission via a network or removable media?**

* All transmission protocols should be secured, if possible

**If data is not encrypted by default, can the customer configure encryption options?**

* If data is not encrypted by default, customer can’t have configure encryption

**Is sensitive data transmission restricted to a fixed list of network destinations?**

* Any data transmitted by the device should utilize approved secure transmission protocols, if possible

**Are connections limited to authenticated systems?**

* Yes, only authenticated users can have access to the systems

# Transmission Integrity

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.

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

* Ensure integrity by creating a digital signature of the message using the sender's private key.
* The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures

# Remote Service

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
* Sensitive data that will not be accessed or viewed from the device during the remote session
* Remote access sessions can be categorized to whether patient data are or can be accessed during a remote servicing session
* Personal data storage should include enhanced security measures and consider full encryption of the data
* Proper identification and authorization of the remote service center at the customer site

# Security Program Integration

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

**Vulnerability Management**

* Implementation of security scanning tools within the organization
* Onboarding the application/infrastructure to the scanning tool
* Identify and prioritization of the vulnerability as per vulnerability rating such as critical, High, Medium, low and information
* Planning the vulnerability remediation and mitigation options
* Tracking and revalidation of the vulnerability remediation and mitigation

**Incident Response**

* Unexpected system behavior
* Suspected malware on the system
* Confirmed malware on the system
* 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**

* Client need to update the software or hardware if needed.
* Client need to test or validate the effectiveness of system security function
* Functional testing should be performed to identify the loop holes

**Scanning**

* Network security scanning and web application vulnerability scanning should be performed to remove the legacy Applications/Devices within infrastructure
* Manual and automated vulnerability scanning of the system should be performed as per the business approval

**Risk Management**

* Client need to conduct security risk management process which monitors the ongoing security posture of this device and addresses any security incidents that might arise.
* Risk assessment should be conducted within the organization to identify the gaps and proves improvements

**Training and Awareness**

* Properly documented manual and devices functioning training should be provided to customers and staff members utilizing the devices
* Client need to evaluate the security training requirements for this product and determined that standard user security and awareness training for business purpose to user.
* Workforce members utilizing medical devices should be appropriately trained.
* Medical device owners or designees should train appropriate workforce members on the use of the medical device to include any issues/concerns related to its use.

# 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**

* Data should be discarded after a period of time example: 6 months
* Access to data should be take away asap the users does not need it
* Access to the devices should be taken away within 24 hours of devices not needed be customers

**What happens to data when the product is reinitialized?**

* Removal of redundant equipment and software

**How to security decommission data when the product is non-functional**

* Removal of any emanation control equipment or security enhancements;

**Whether decommissioning can happen locally or remotely**

* Decommission should happen only after the device is handed over

**Whether and how to remove sensitive data before product is serviced**

* Return or safe disposal of any emanation control equipment or security enhancements;
* Updates to systems configurations (switches, firewalls etc.);
* Equipment and media sanitization including any cloud-based data & services (discussed later in this chapter);
* Equipment and media disposal (discussed later in this chapter);
* Any legal considerations for supply or service contract terminations;