

**Smartmedic™ Device**

**Security Operations Manual**



~~REF: 6007-670-000~~



**Table of Contents**

[01 Purpose 1](#_Toc96001785)

[02 Definitions 1](#_Toc96001786)

[03 Product Description 3](#_Toc96001787)

[3.1 Device and Manufacturer Identification 4](#_Toc96001788)

[3.4 System Characterization and System Assets 5](#_Toc96001789)

[3.5 System Security Context and Intended Environment 5](#_Toc96001790)

[04 Automatic Log-Off 6](#_Toc96001791)

[05 Audit Controls 6](#_Toc96001792)

[06 Authorization 9](#_Toc96001793)

[6.1 Access Prevention 10](#_Toc96001794)

[6.2 Privilege and Access 10](#_Toc96001795)

[6.3 System Use Notification 11](#_Toc96001796)

[07 Cyber Security Product Upgrades 11](#_Toc96001797)

[7.1 Secure Servicing and Security Upgrades Overview 11](#_Toc96001798)

[7.2 General Parameters for Updates 11](#_Toc96001799)

[7.3 Operating System Updates 12](#_Toc96001800)

[7.4 Driver, Firmware Updates 12](#_Toc96001801)

[7.5 Anti-Malware Software Updates 13](#_Toc96001802)

[7.6 COTS (non-OS) Updates 13](#_Toc96001803)

[7.7 Other Software Component Updates 14](#_Toc96001804)

[7.8 Data Backup and Disaster Recovery 14](#_Toc96001805)

[08 Health Data Integrity and Authenticity 14](#_Toc96001806)

[09 Malware Detection/Protection 15](#_Toc96001807)

[09.1 Other Compensation/Protection Controls 15](#_Toc96001808)

[09.2 Support of Anti-Malware 15](#_Toc96001809)

[10 Connectivity Capabilities 16](#_Toc96001810)

[10.1 Hardware Connectivity Capabilities (CONN-1) 16](#_Toc96001811)

[10.2 Other Compensation/Protection Controls 16](#_Toc96001812)

[11 Personal Authentication 17](#_Toc96001813)

[11.1 Password/ID Assignments 17](#_Toc96001814)

[11.2 Other Compensation/Protection Controls 17](#_Toc96001815)

[12 Physical Locks 18](#_Toc96001816)

[13 Roadmap for Third Party Components in Device Life Cycle 19](#_Toc96001817)

[14 System and Application Hardening 19](#_Toc96001818)

[15 Health Data Storage Confidentiality 21](#_Toc96001819)

[16 Transmission Confidentiality 21](#_Toc96001820)

[17 Transmission Integrity 22](#_Toc96001821)

[18 Remote Service 22](#_Toc96001822)

[19 Security Program Integration 23](#_Toc96001823)

[20 Secure Decommissioning 24](#_Toc96001824)

# 01 Purpose

This Security Operations Manual (SOM) provides information that Stryker’s customers need to know in order to integrate a specific Stryker device or health IT solution into a customer’s IT network environment in a secured manner.

It also supports customer’s ability to perform risk management, to identify configurable security controls, and to better protect their systems.

# 02 Definitions

**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.

**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.

Refer 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 (for example, IEC 62304).

Refer 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.

**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 (for example, ISO/IEC 27034). Refer 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.

Refer https://ec.europa.eu/health/md\_sector/overview\_en

**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**

Refer 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).

Refer 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 the following:

Any information that can be used to distinguish or trace an individual’s identity.

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.

**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.

# 03 Product Description

This Security Operations Manual (SOM) provides information that Stryker’s customers need to know in order to integrate a specific Stryker device or health IT solution into a customer’s IT network environment in a secured manner.

It also supports customer’s ability to perform risk management, to identify configurable security controls, and to better protect their systems.

|  |  |
| --- | --- |
| **Manufacturer Name** |  |
| **Stryker Division** | Stryker Global Technology Center |
| **Address** | **Stryker Global Technology Center Private Limited**  10th Floor, Vatika Business Park,  Block Two, Sector-49 ,Sohna Road,  Gurgaon 122002, Haryana, India |
| **Device Description** | Smartmedic Device is used to monitor the health vital data i.e weight, temperature, position. The Smartmedic Device is intended to provide an alert for the unwanted change the health vital, that uses the device’s sensor data to visualize the current health condition of patient in the real time to enable effective decision making for the health personal before they even go into the operating room on the daily health inspection. |
| **Device Model, Version** | **~~6007-670-000 V1.0 (Further digits for minor fixes controlled internally)~~** |
| **Manufacturer Contact**  **Information** | **Manufacturer:**  **Stryker Global Technology Center Private Limited**  10th Floor, Vatika Business Park, Block Two, Sector-49, Sohna Road, Gurgaon 122002, Haryana, India  **Distributed By**:  **Stryker Japan K.K**.  2-6-1, Koraku, Bunkyo-ku,Tokyo, 112-004, Japan t/f: 03-6894-0000  Additional information and contact links are available on Stryker’s Product Security webpage, https://www.stryker.com/us/en/about/governance/cyber-security.html. |

*Table 1.1 Product Description*

## 3.1 Device and Manufacturer Identification

**Device**

Smartmedic Device

**Manufacturer**

**Stryker Global Technology Center Private Limited**

10th Floor, Vatika Business Park

Block Two, Sector-49, Sohna Road,

Gurgaon 122002, Haryana, India

**3.2 Device Intended Use**

Smartmedic Device used to monitor the health vital data i.e weight, temperature, position. The Smartmedic Device intended to provide an alert for the unwanted change the health vital, which uses the device’s sensor data to visualize the current health condition of patient in the real time to enable effective decision making for the health personal before they even go into the operating room on the daily health inspection.

Functionality Includes:

* Monitor the health vital data i.e weight, temperature, position
* Device provide an alert for the unwanted change the health vital.
* Device’s sensor data to visualize the current health condition of patient in the real time.
* Visualize the current health condition of patient in the real time.
* Enable effective decision making for the health personal

**3.3 Vulnerability Intake and Monitoring**

When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact conducted. Based upon the 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.

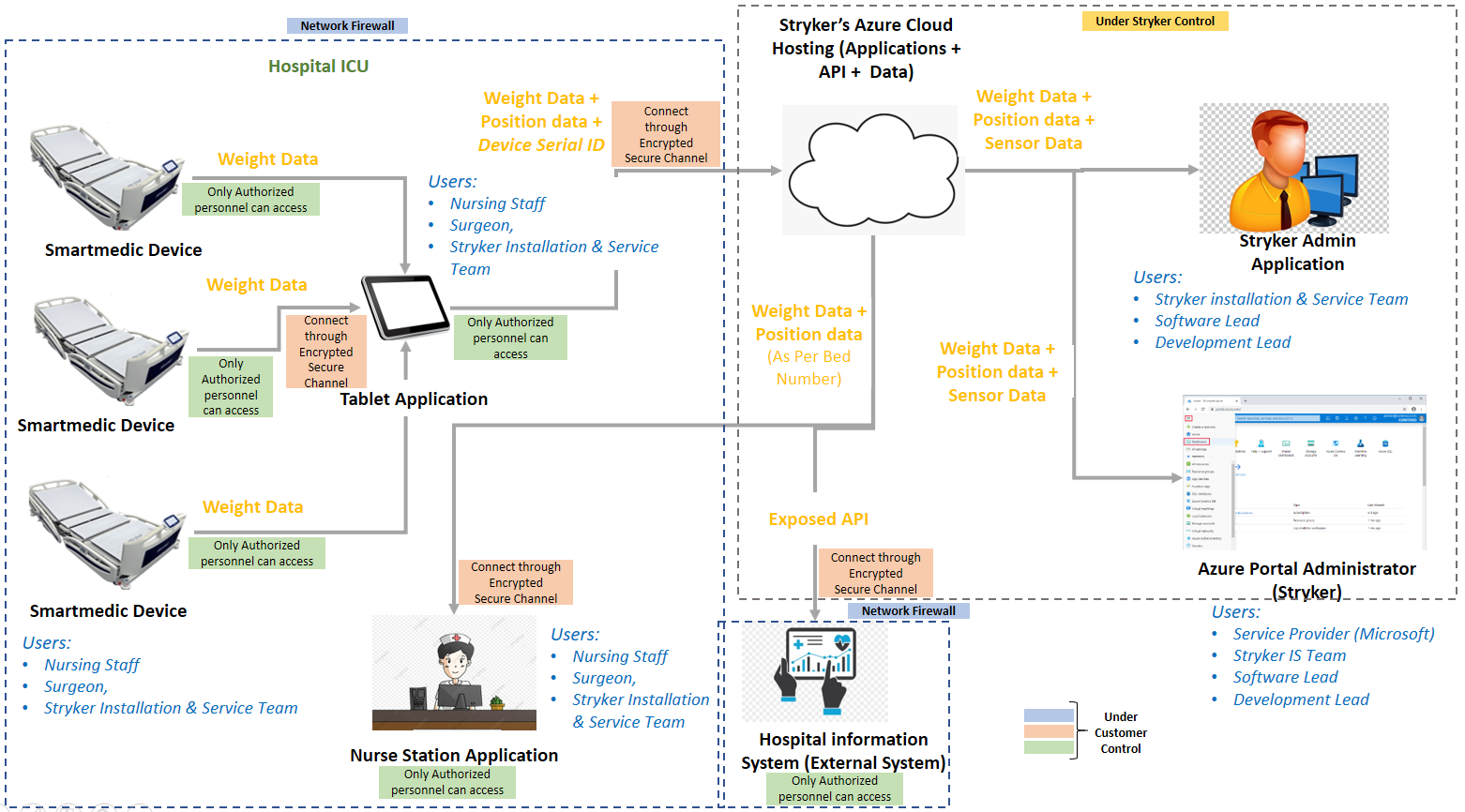
Any potential security vulnerabilities customer may become aware of due to Smartmedic Device must be communicated to Stryker customer care and the same will be handled through the post market complaints management process to do the assessment and required actions including any updates needed for the customers.

## 3.4 System Characterization and System Assets

Smartmedic Device used to monitor the health vital data i.e weight, temperature, position. The Smartmedic Device intended to provide an alert for the unwanted change the health vital, which uses the device’s sensor data to visualize the current health condition of patient in the real time to enable effective decision making for the health personal before they even go into the operating room on the daily health inspection. This device only allowed for sending data and information to Smartmedic tablet further send data to the Stryker cloud storage for further analysis. This device will not be allow user to transfer the patient data to any other external or connected system to process further. All the patient data encrypted and stored locally and cloud under the particular logged user and hospital entity.

## 3.5 System Security Context and Intended Environment

**For the Context for Stryker’s End Customers’**

**

*Figure 1: System Security*

While there is no specific requirement for Smartmedic Device to be fully functional other than a usual good network security and communication tools environment, however Stryker recommends the user to follow some of the best practice security standards in order to run the application in a safe and secure environment as follows:

Devices operating in the intended use environment should consider that their IT infrastructure must follow different risk management approaches associated with their networks. HDO or customer must adopt a risk management process adhering to general cybersecurity best practices to maintain the healthcare provider’s overall security status and their secure environment, as follows:

* Good physical security to prevent unauthorized physical access to Smartmedic Device application.
* Access control measures (for example, role based) to ensure only authenticated and authorized personnel are allowed access to network elements, stored information, services and applications.
* Device communication should be in the encrypted secure channel.
* General patch management practices that ensure timely security patch updates.
* Malware protection to prevent unauthorized code execution.
* Use the good network security and communication tools.
* Security awareness training.

# 04 Automatic Log-Off

**For the Context for Stryker’s End Customers’**

Stryker’s Customers are advised to configure android OS to automatically lock the screen after a period of idle time as per the HDO IT policies.

Application also has the ability to lock the screen after inactivity for configurable timeout. User can configure the inactivity timeout. For details, please refer User Manual Section to configure System Settings. Customer should setup the length of inactivity time before auto-logoff screen, device screen saver should be activated for idle period of time.

# 05 Audit Controls

**For the Context for Stryker and Stryker’s End Customers’**

Stryker uses strong protection mechanism to protect the audit logs from being tampered by any unauthorized party and hence does not require any extra steps from the users. Audit logs are encrypted using MQTT Protocal, 256-bit AES encryption to avoid any tampering of the information. Stryker handles decryption of the audit log on request from authorities. User cannot edit or alter the audit logs.

Smartmedic Device captures the following type of audit events:

* Creation/modification events of sensitive data (No PII data stored)
* MQTT Protocol used for secure communication between Smartmedic device, tablet, cloud and system.
* Marked data with time stamp information to enable it to be selected for deletion based on when it was acquired or stored. Work step visited, save / update operation on patient health vital data. Application data - workflow and features executed.
* Maintain server security logs
* Maintain access logs

Audit Logs Format is: <timestamp>,<user>,<component>,<Feature/Module>,<Action>

It is possible to export the logs via physical media considering the physical media like USB etc. to be secure. However, it is recommended for the users to keep their physical media secure and updated against the latest threats.

Below are some of the safety measures that can be implemented to secure physical media like USB drive.

**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 recorded in the audit log indicate which of the following events recorded in the audit log:

Successful login/logout attempts

* Authorized user should have access to the device
* Role based access controls should be provided to each users accessing the device ex: Doctor, Nurse, Admin Users etc.
* 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.

T

he 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.

**Do not plug a USB drive into an unknown computer**

Do not plug the USB into any computer without verifying the identity and safety of that computer system as the system may pose a potential security threat to your physical device.

**Take advantage of security features**

Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.

**Disable Autorun**

The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. Disabling Autorun prevents malicious code on an infected USB drive from opening automatically.

**Use and maintain security software and keep all software up to date**

Use a firewall, antivirus software, and anti-spyware software to make your computer less vulnerable to attacks and keep the virus definitions current. Also, keep the software on your computer up to date by applying any necessary patches.

# 06 Authorization

**For the Context for Stryker’s End Customers’**

Smartmedic Device requires a valid authorization in order to be operational, functional, running and continuous health monitoring the device user must leverage android authentication and authorization mechanism for user access to software and data. So, Stryker best recommends the user to setup proper authorization of users on the tablets as discussed below.

Authorization in system security is the process of giving the user permission to access a specific resource or function. In secure environments, authorization must always follow authentication. Users should first prove that their identities are genuine before an organization’s administrators grant them access to the requested resources. So proper authorization must be implemented at system level to harden the security. Different approaches to authorization may include

**Role-Based Access Control (RBAC)**

Users identified as being in a role that stipulates what privileges they have. Additionally, their user ID would restrict what data they have access to.

**Access Control Lists (ACL)**

An ACL specifies which users have access to particular resources. For instance, if a user wants to access a specific file or folder, their username or details should be mentioned in the ACL in order to be able to access certain data.

## 6.1 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.

## 6.2 Privilege and Access

Stryker recommends the IT administrator to create separate users with appropriate privileges for access to Smartmedic device on the same tablet/system. Privilege and access to the Smartmedic device must be restricted such that any user of the device can only use it within its intended use and any other functionality outside of the scope of the application is restricted as much as it can be. Users can maintain their own data on tablet/device/system without access to other user’s data by setting different log in 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.

## 6.3 System Use Notification

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

**Users can be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service,**

# 07 Cyber Security Product Upgrades

The Device does not have any updates installation policy implemented. Hence, the users will not get any online updates. If Stryker identifies any potential vulnerabilities, which require an update at the customer site, a new version of the software will be released, and customers will be informed about the action to be taken at their end.

It is HDO’s responsibility to update the latest patches for their operating system, their third-party components (if any) and other applications like Virus Protection software’s/anti-malware software’s, firewalls etc. Timely to ensure the security and protection of the system.

Smartmedic Device contain malware protection embedded within Smartmedic device. Hence, users are advice to install and anti-malware software on laptop.

## 7.1 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, hardware, or firmware.
* Customer need to update the third-party software or firmware if needed.

## 7.2 General Parameters for Updates

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

* Customer notified when updates approved for installation
* Customer can be provided automatic installation of software updates
* Approved list of third-party software that can be installed on the device by Stryker engineer whenever needed allowed for the Smartmedic device.
* Owner/operator of manufacturer-approved third-party software should be install on device.
* HDO IT Administrator can make policy to prevent installation of unapproved software
* Stryker will review and approval status of updates
* Stryker and Customer can make combined review cycle for the device

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

## 7.3 Operating System Updates

Stryker will provide 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.

Stryker’s will provide authorized service to install patches or software updates

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 (e.g., Microsoft) 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

## 7.4 Driver, Firmware Updates

Stryker will provide 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

Stryker will provide authorized service to install patches or software updates

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 (e.g., Microsoft) 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 .

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

## 7.5 Anti-Malware Software Updates

Stryker will provide 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

Stryker will provide authorized service to install patches or software updates

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 (e.g., Microsoft) 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

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

## 7.6 COTS (non-OS) Updates

Stryker will provide 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

Stryker will provide authorized service to install patches or software updates

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 (e.g., Microsoft) 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

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

## 7.7 Other Software Component Updates

Stryker will provide 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

Stryker will provide authorized service to install patches or software updates

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 (e.g., Microsoft) 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

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

## 7.8 Data Backup and Disaster Recovery

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

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

# 08 Health Data Integrity and Authenticity

No user actions are needed since any health data or other sensitive data stored on the system is encrypted using strong 256-bit AES encryption algorithm by the application itself to preserve the data integrity. The application properly checks the integrity of the data before loading them.

Stryker will handle data integrity checking mechanisms of stored health data (e.g., hash or digital signature).

* Hashing algorithm, 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

# 09 Malware Detection/Protection

The standalone Smartmedic Device by default contains any malware detection functionality. As, the malware detection is crucial with malware’s prevalence because it functions as an early warning system for the computer secure regarding malware and cyberattacks. It keeps hackers out of the computer and prevents the information from getting compromised. This involves the process of scanning the computer and files to detect malware.

## 09.1 Other Compensation/Protection Controls

The Smartmedic Device application contains several protection mechanisms by its design like the device requires a valid authorization in order to work properly, the logs are encrypted using private keys and the data de-identification is also done which anonymizes the data at runtime.

## 09.2 Support of Anti-Malware

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.

Stryker’s operator to install or update anti-malware software

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

Stryker’s 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 (e.g., Microsoft) need to upgrade the software and firmware.

* Client 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.

Malware notifications written to a log

*IPS or IDS or SIEM tool should be implemented in organization***Other things to consider:**

* It is imperative that logs/warnings get the attention of the user. Any anomaly must then be resolved after its addressed.
* Ensure that ports necessary for function are accessible only to authorized clients of the device.
* In case a malware was reported on the system, ensure a proper sweep scan has been initiated and the removal of the malware was successful before resuming normal operations.

Firewall helps in preventing network access to devices. If properly used and configured it can lead to protected and reliable accessibility. It can help in prevention of unauthorized access and network connections against external threats, IP spoofing & routing attacks and malicious packets.

# 10 Connectivity Capabilities

**For the Context for Stryker’s End Customers’**

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.

## 10.1 Hardware Connectivity Capabilities (CONN-1)

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

:

## 10.2 Other Compensation/Protection Controls

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 Stryker 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.

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.

# 11 Personal Authentication

The ability to configure the device to authenticate users.

## 11.1 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

## 11.2 Other Compensation/Protection Controls

**For the Context for Stryker’s End Customers’**

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

* Email validation to verify the identity
* OTP code to change the password
* Secret questions to change the password

Configuration to enforce creation of user account passwords that meet established (organization specific) complexity rules

Support of any account passwords that expire periodically

* Password changes should be auto enable after 180 days

Support of multi-factor authentication

* 2FA can be enabled to get the code via Voice, message or email

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

# 12 Physical Locks

**For the Context for Stryker’s End Customers’**

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.

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

Stryker’s end Customers’ need to ensure the physical security of the device.

# 13 Roadmap for Third Party Components in Device Life Cycle

Stryker has evaluated third -party components as per the requirement identified in IEC 62304 and adequate actions are implemented in application.

Stryker will be evaluating high-risk third-party components periodically and communicate to customers for any updates required during the product lifecycle.

# 14 System and Application Hardening

Stryker had performed the system and application security testing and security code review of Smartmedic Device. Smartmedic Device is hardened by eliminating any vulnerability or flaw, which can lead to security issue.

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in the application, systems, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system’s attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, so on. attackers and malware have fewer opportunities to gain a foothold within the IT ecosystem. Systems hardening demands a methodical approach to audit, identify, close, and control potential security vulnerabilities. The type of hardening carried out depends on the risks in the existing technology, the resources that are available, and the priority for making fixes.

Stryker recommends to customers to keep below key points while implementing the system hardening.

**Audit your existing systems**

Carry out a comprehensive audit of the existing technology. Use penetration testing, vulnerability scanning, configuration management, and other security auditing tools to find flaws in the system where the application is installed and prioritize fixes

**Create a strategy for systems hardening**

There is no need to harden all the systems at once. Instead create a strategy and plan based on risks identified within the technology ecosystem and use a phased approach to remediate the biggest flaws.

**Patch vulnerabilities immediately**

Ensure to have an automated and comprehensive vulnerability identification and patching system in place.

**Network hardening**

**For the Context for Stryker’s End Customers’**

Ensure the firewall is properly configured and that all rules are regularly audited; secure remote access points and users; block any unused or unneeded open network ports; disable and remove unnecessary protocols and services; implement access lists; encrypt network traffic.

* Wi-Fi (consider authentication protocols supported, such as WPA2 EAP-TLS)
* Bluetooth (consider security modes supported)

**Operating system hardening**

Apply OS updates, service packs, and patches automatically; remove unnecessary drivers, file sharing, libraries, software, services, and functionality; encrypt local storage; tighten registry and other systems permissions; log all activity, errors, and warnings; implement privileged user controls.

**Eliminate unnecessary accounts and privileges**

**For the Context for Stryker’s End Customers’**

Enforce least privilege by removing unnecessary accounts (such as orphaned accounts and unused accounts) and privileges throughout the IT infrastructure.

**Anti-Malware installation**

The system running Smartmedic Device should have proper anti-malware software installed with latest updates.

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

* Yes, Devices is always Hardened beyond the default state

**Are instructions available from Stryker for increased hardening?**

* Yes, whenever needed.

**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?**

**For the Context for Stryker’s End Customers’**

* 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)

# 15 Health Data Storage Confidentiality

The data at rest is encrypted using a strong encryption mechanism implemented within the application, which safeguards the sensitive medical data from prying eyes.

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.

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 should be used
* Customer instruction to configure encryption

Change or configuration instruction of encryption keys whenever Stryker has provided the same.

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.

# 16 Transmission Confidentiality

**For the Context for Stryker and Stryker’s End Customers’**

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

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

Sensitive data be transmitted only via a point-to-point dedicated channel

* 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

Sensitive data encrypted prior to transmission via a network or removable media

* All transmission protocols should be secured, MQTT

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

* If data is not encrypted by default, customer can’t have configure encryption using the secure channel of communication

Sensitive data transmission restricted to a fixed list of network destinations?

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

Are connections limited to authenticated systems?

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

Secure transmission methods supported/implemented.

* Wi-Fi (consider authentication protocols supported, such as WPA2 EAP-TLS)
* Bluetooth (consider security modes supported)

# 17 Transmission Integrity

The ability of the device to ensure the integrity of transmitted data. 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 and wireless connection,

* 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

# 18 Remote Service

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

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
* Indication to enable and active remote session
* Patient data that will 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

Permits or uses remote service connections for predictive maintenance data, specify the connections.

Device has any other remotely accessible functionality (e.g., software updates, remote training)

# 19 Security Program Integration

The secure practices for the device/software covered under Section 7 of this document.

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

* 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

* 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

**For the Context for Stryker and Stryker’s End Customers’**

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.

# 20 Secure Decommissioning

**For the Context for Stryker and Stryker’s End Customers’**

Please reach out to Stryker Customer Care for secured decommissioning.

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 data of equipment and software

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

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

***Stryker Corporation or its divisions or other corporate affiliated entities own, use or have applied for the following trademarks or service marks: Smartmedic Device, Triathlon. All other trademarks are trademarks of their respective owners or holders.***



**Stryker Global Technology Center Private Limited**

Vatika Business Park, 10th Floor

Block 2, Sector-49

Sohna Road

Gurgaon 122002

Haryana

India

www.stryker.com

*Copyright © 2022 Stryker*