

**SmartMedic™**

**Security Operations Manual**



~~REF: 6007-670-000~~



**Table of Contents**

[01 Purpose 1](#_Toc96438160)

[02 Definitions 1](#_Toc96438161)

[03 Product Description 2](#_Toc96438162)

[3.1 Device and Manufacturer Identification 3](#_Toc96438163)

[3.2 Device Intended Use 3](#_Toc96438164)

[3.3 Vulnerability Intake and Monitoring 4](#_Toc96438165)

[3.4 System Characterization and System Assets 4](#_Toc96438166)

[3.5 System Security Context and Intended Environment 4](#_Toc96438167)

[04 SmartMedic Solution’s components 5](#_Toc96438168)

[4.1 SmartMedic: Device 6](#_Toc96438169)

[4.2 SmartMedic: Tablet 6](#_Toc96438170)

[4.3 SmartMedic: Nurse Station Application 8](#_Toc96438171)

[4.4 SmartMedic: Cloud Application 8](#_Toc96438172)

[4.5 SmartMedic: Communication Network 8](#_Toc96438173)

# 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.

**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.

**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.

**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.

**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).

**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.

**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 Stryker’s SmartMedic 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 solution 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 Solution used to monitor the health vital data i.e weight, temperature, position. The SmartMedic Device intended to provide an alert for the unexpected 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
* SmartMedic solution provide an alert for the unexpected changes in 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

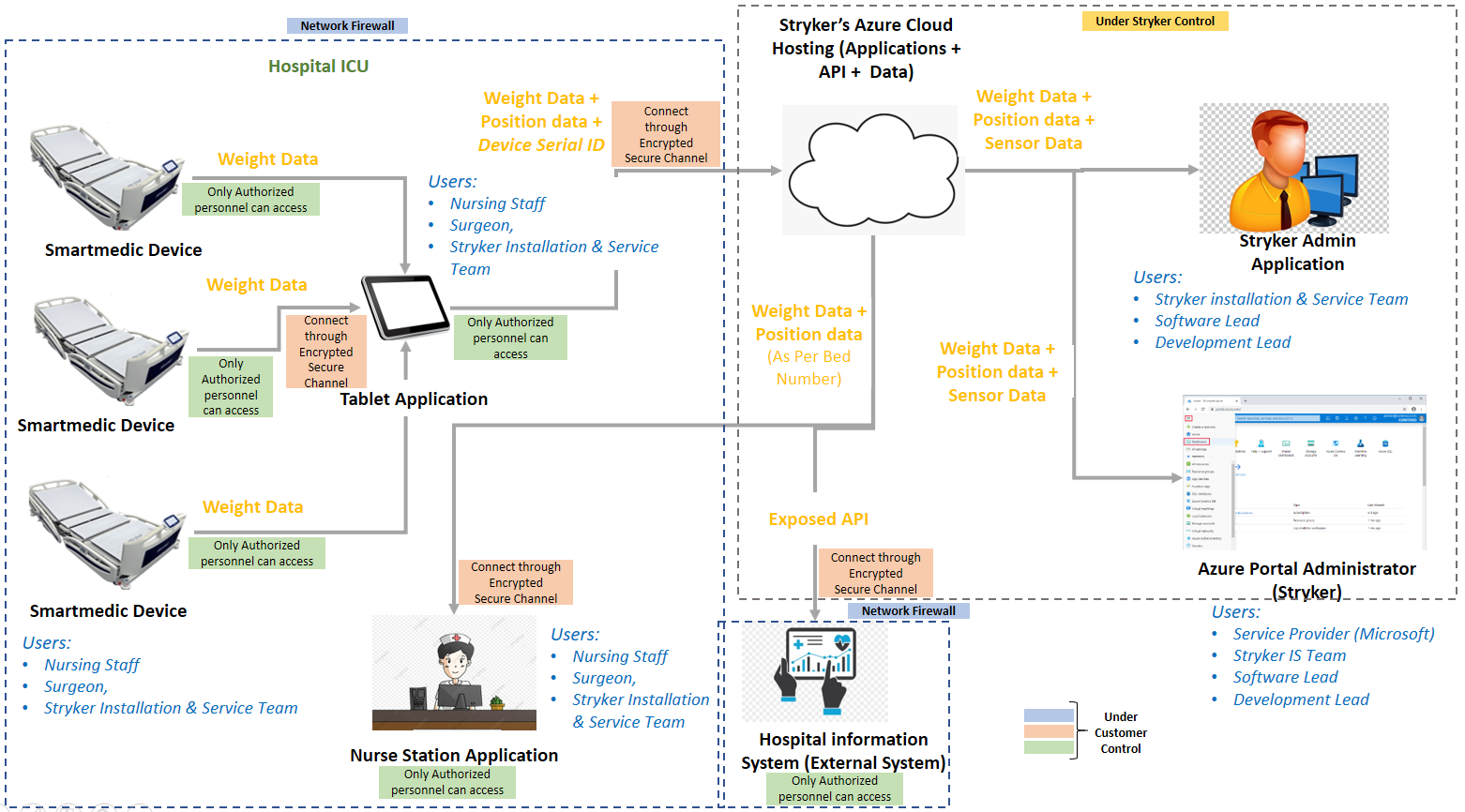
When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact conducted. Based upon the assessment Stryker determines if further actions are required like, providing security updates and/or providing communication 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 Solution used to monitor the health vital data i.e weight, temperature, position. The SmartMedic Device intended to provide an alert for the unexpected 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 solution’s tablet that further sends data to the Stryker cloud storage for further analysis. This device will not allow user to transfer the patient data to any other external or connected system to process further. The patient data encrypted and stored locally and cloud under the particular logged user hospital entity.

## 3.5 System Security Context and Intended Environment

**

*Figure 1: System Security*

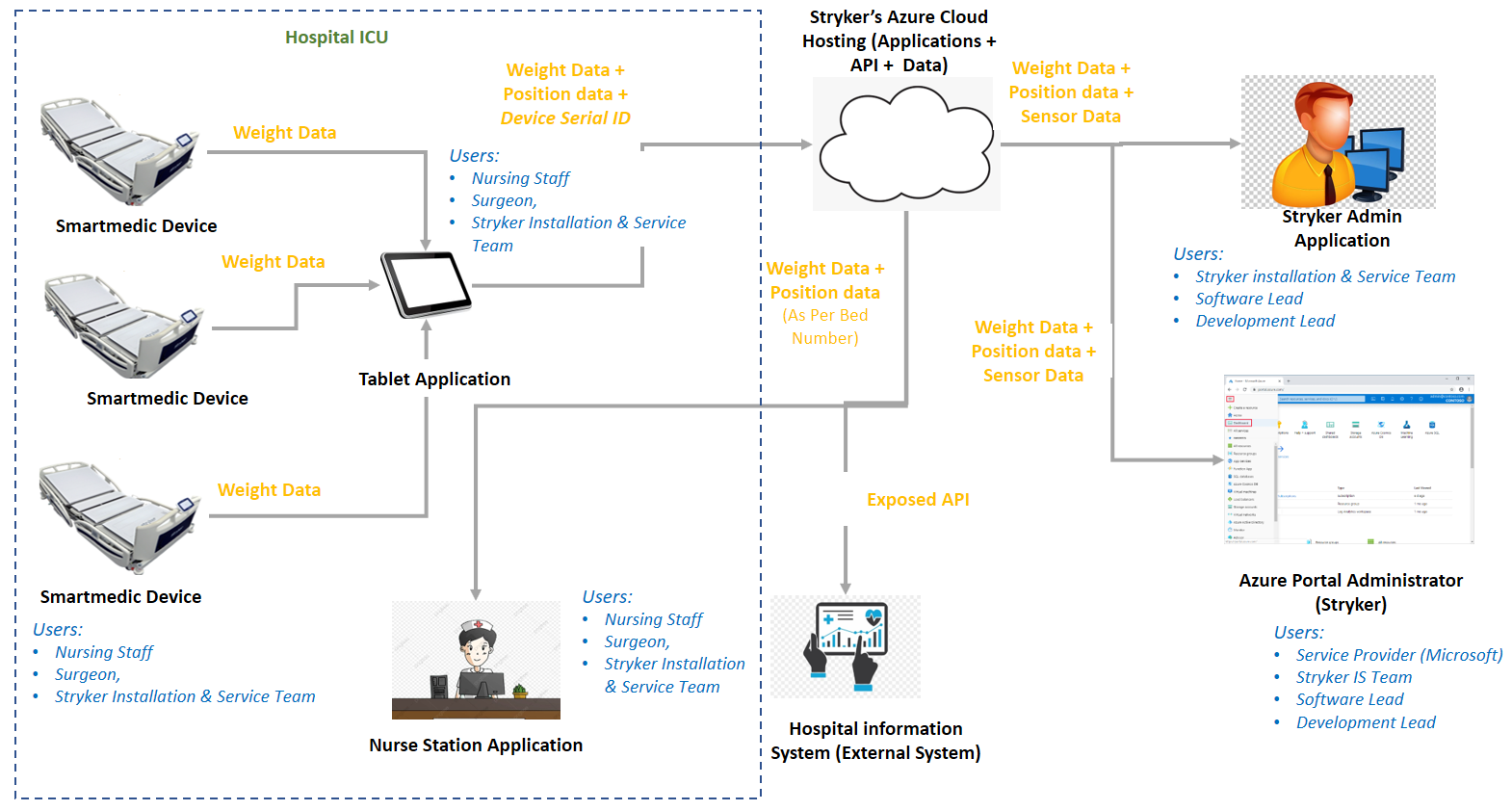
While there is specific requirement for SmartMedic solution to be a usual good network security and communication tools environment, however Stryker recommends the user to follow the best practice security standards in order to run the SmartMedic solution in a safe and secure environment as follows:

Devices operating in the intended use environment should consider that their IT infrastructure must follow different risk management approaches associated with their networks. Some recommendations are:

* Good physical security to prevent unauthorized physical access to SmartMedic Device application.
* Access control measures to ensure only authenticated and authorized personnel are allowed access to network elements, stored information, services and applications.
* Communication between SmartMedic solution’s tablet and SmartMedic application should be in the encrypted secure channel.
* General patch management practices that ensure timely security patch updates.
* Use the good network security and communication tools.
* Security awareness training.

# 04 SmartMedic Solution’s components

SmartMedic Solution used to monitor the health vital data such as weight, temperature, position etc. The SmartMedic Device intended to provide an alert for the unexpected change the health vital.



SmartMedic Solution’s components:

* SmartMedic: Device
* SmartMedic: Tablet
* SmartMedic: Nurse Station Application
* SmartMedic: Main Application
* SmartMedic: Communication Network

## 4.1 SmartMedic Solution Component: Device

SmartMedic device consist of the sensors that are used to monitor the health vital data such as weight, temperature, position. This device only allowed for sending data and information to SmartMedic solution’s tablet.

**Existing Security Features**

**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 solution will released, and customers will informed about the action to be taken at their end. SmartMedic solutions contain malware protection embedded within SmartMedic tablet. Tablet also contains authorized service to install patches or software updates. Stryker has ability to recover after damage or destruction of device data, configuration information.

**Security Program Integration:**

Stryker will take care of the scanning, security testing, and vulnerability management of SmartMedic solution’s components

**Customer Need to Consider**

**Secure Decommissioning:**

Please reach out to Stryker Customer Care for secured decommissioning.

## 4.2 SmartMedic: Tablet

SmartMedic solution’s tablet that further sends sensor data to the Stryker cloud storage for further analysis. The tablet collects the sensor data from all the smart medic devices which of them are configured to send the data.

**Existing Security Features**

**Automatic Log-Off:**

Stryker has preconfigured the automatic Log-Off for the tablet.

**Authorization:**

Only Stryker’s service engineer authorized to access the SmartMedic solutions component like tablet etc. Whenever needed at the time of maintenance.

**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. Only Stryker Technical Team authorized to repair or resolve issue whenever severe malware has been detected.

**Roadmap for Third Party Components in Device Life Cycle:**

Stryker has evaluated third -party components as per the requirement identified 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.

**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.

**Security Program Integration:**

Stryker will manage the scanning, security testing, and vulnerability management of SmartMedic solution’s components

**Health Data Storage Confidentiality:**

The data at rest encrypted using a strong encryption mechanism implemented within the SmartMedic solution, 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 sensitive information stored on the device.

**Customer Need to Consider**

**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.

* All device components maintain sensitive data physically secure (i.e., cannot be removed without tools), 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.

**System and Application Hardening:**

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)

**Secure Decommissioning:**

Please reach out to Stryker Customer Care for secured decommissioning.

## 4.3 SmartMedic: Nurse Station Application

SmartMedic: Nurse Station Applications get an alert for the unexpected 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.

**Existing Security Features**

**Personal Authentication:**

Stryker’s customer only authorized to access the Nurse Station web application. The Stryker will provide the personal authentication credential for the same. Stryker’s customer can access the Nurse Station web application using the credentials provided by the Stryker.

**Security Program Integration:**

Stryker will take care of the scanning, security testing, and vulnerability management of SmartMedic solution’s components

## 4.4 SmartMedic: Main Application

SmartMedic: Main Application used to collect sensor data, monitor the health vital data i.e weight, temperature, position. The application can also perform the analysis over the received data to provide an alert for the unexpected change the health vital, which uses the device’s sensor data to visualize the current health condition of patient in the real time.

**Existing Security Features**

**Audit Controls:**

Stryker uses strong protection mechanism to protect the audit logs and the required audit logs are maintained by Stryker.

**Health Data Integrity and Authenticity:**

SmartMedic solution will manage data integrity checking mechanisms of stored health data.

**Security Program Integration:**

Stryker will manage the scanning, security testing, and vulnerability management of SmartMedic solution’s components

## 4.5 SmartMedic: Communication Network

SmartMedic: communication network used to transmit the information from the source to the destination.

**Existing Security Features**

The ability of the SmartMedic solution ensure the confidentiality of transmitted sensitive information. Transmits sensitive data only via a point-to-point dedicated channel between SmartMedic device and Tablet.

**Customer Need to Consider**

**Health Data Integrity and Authenticity:**

SmartMedic solution will handle data integrity checking mechanisms of stored health data. Customer only need to provide the secure encrypted channel for the communication between the SmartMedic solution’s component i.e. the tablet and Stryker main application.

**Malware Detection/Protection:**

Whenever severe malware has been detected and got resolved by the service engineer. Customer has to blocks the few IOCs and IOAs at their network devices. 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.

**Connectivity Capabilities:**

All network connections must be considered in determining appropriate security controls. The customer will provide the secure encrypted channel such as wireless connection like Wi-Fi (consider authentication protocols supported, such as WPA2 EAP-TLS) for the communication between the SmartMedic solution’s components i.e. the tablet and Stryker cloud. SmartMedic solution uses the strong secure communications protocol for communicating among the components.

***Stryker Corporation or its divisions or other corporate affiliated entities own, use or have applied for the following trademarks or service marks: SmartMedic Solution. 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*