

**SmartMedic™**

**Security Operations Manual**



~~REF: 6007-670-000~~



**Table of Contents**

[01 Purpose 3](#_Toc97853151)

[02 Definitions 3](#_Toc97853152)

[03 Product Description 4](#_Toc97853153)

[3.1 Device and Manufacturer Identification 5](#_Toc97853154)

[3.2 Device Intended Use 5](#_Toc97853155)

[3.3 Vulnerability Intake and Monitoring 6](#_Toc97853156)

[3.4 System Characterization and System Assets 6](#_Toc97853157)

[3.5 System Security Context and Intended Environment 6](#_Toc97853158)

[3.6 Smart Medic Solution’s Component 7](#_Toc97853159)

[04 User Account Management 7](#_Toc97853160)

[05 Access control policy and management 8](#_Toc97853161)

[06 Security Awareness Training 8](#_Toc97853162)

[07 Incident Management, Response, Training, Testing, Handling, Monitoring & Reporting 8](#_Toc97853163)

[08 Contingency Plan: Testing, Maintenance and Training 9](#_Toc97853164)

[09 Trustworthiness- CIA Triad & Their Responsibilities 10](#_Toc97853165)

[10 System Maintenance 10](#_Toc97853166)

[11 Configuration settings 10](#_Toc97853167)

[12 System and information integrity 11](#_Toc97853168)

[13 Malicious code protection 11](#_Toc97853169)

[14 Information system monitoring 12](#_Toc97853170)

[15 Information handling and retention 12](#_Toc97853171)

[16 Transmission confidentiality and integrity 12](#_Toc97853172)

[17 Security Alerts, Advisories, and Directives 13](#_Toc97853173)

[18 Flaw remediation & Vulnerability Management 13](#_Toc97853174)

[19 Cyber Security Product Upgrades 13](#_Toc97853175)

[20 Security Program Integration 14](#_Toc97853176)

[21 Secure Decommissioning 14](#_Toc97853177)

[22 Cryptographic Protection & Management 14](#_Toc97853178)

[23 Malware Detection/Protection 14](#_Toc97853179)

[24 Roadmap for Third Party Components in Device Life Cycle 15](#_Toc97853180)

[25 Health Data Storage Confidentiality 15](#_Toc97853181)

[26 System and Application Hardening 15](#_Toc97853182)

[27 Physical Locks 16](#_Toc97853183)

# 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 the 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**

“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 as 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 Stryker’s SmartMedic solution into a customer’s IT network environment in a secured manner.

It also supports the 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 unwanted change in the health vital data, that uses the device’s data to visualize the current health condition of the patient in real time. This enables effective decision making for the health personnel before they even go into the operating room -for 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 is used to retrieve the health vital data i.e., weight, position etc. The SmartMedic Device is intended to provide an alert for any unexpected change in the health vitals, and uses the device’s data to visualize the current health condition of the patient in real time. This enables effective decision making for the health personnel before they even go into the operating room for the daily health inspection.

Functionality Includes the following:

* Retrieve the health vital data i.e. weight, position etc.
* SmartMedic solution provides an alert for the unexpected changes in the health vital.
* Device’s data used to visualize the current health condition of patient in the real time.
* Visualize the current health condition of the patient in real time.
* Enable effective decision making for the health personnel

## 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 is 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 by Stryker at any time.

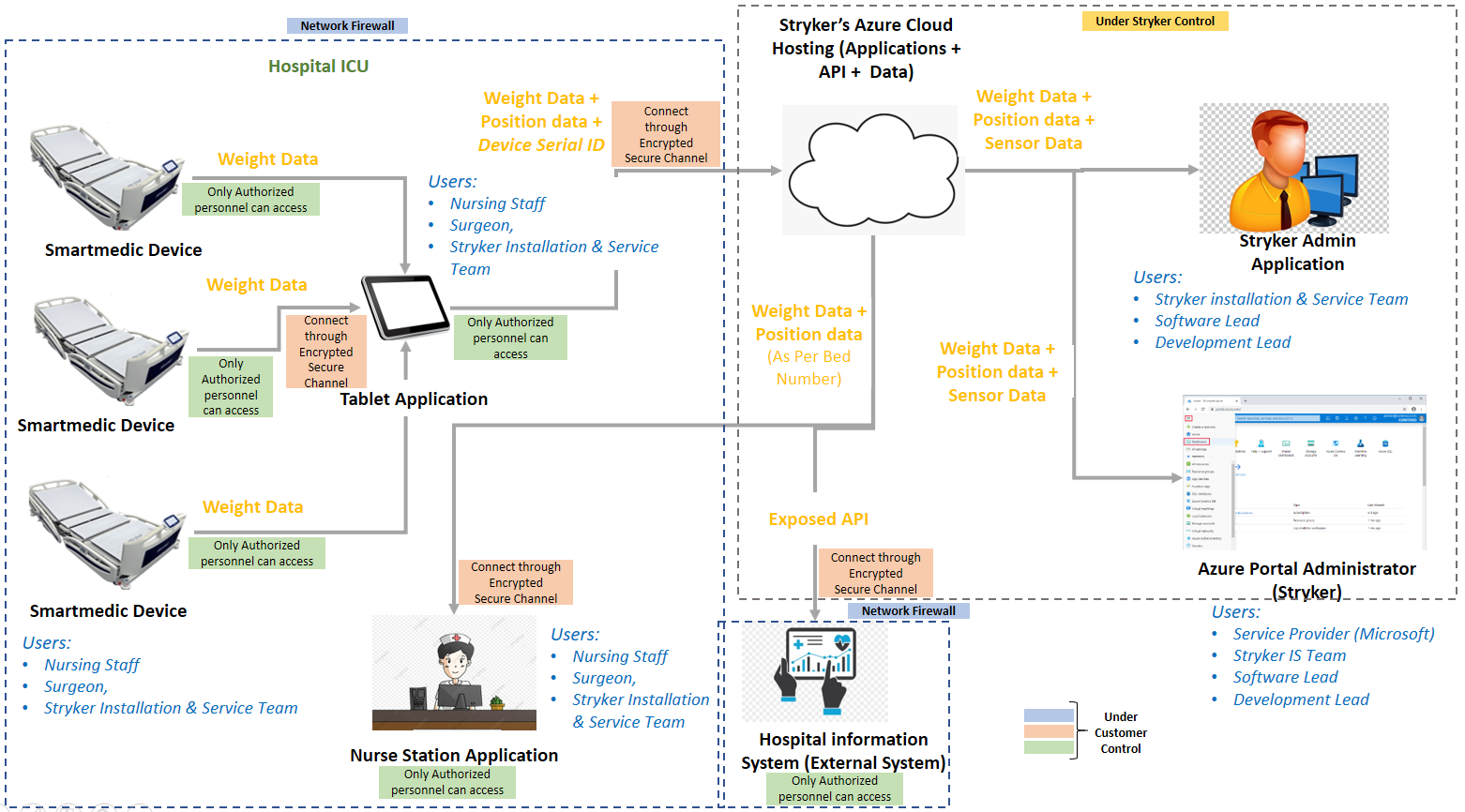
Any potential security vulnerabilities that the customer may become aware of due to SmartMedic Device must be communicated to Stryker customer care and the same will be handled through the post market complaints management process to do the assessment and take required actions including any updates needed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

## 3.4 System Characterization and System Assets

SmartMedic Solution is used to retrieve the health vital data i.e., weight, position etc. The SmartMedic Device is intended to provide an alert for any unexpected change in the health vitals, and uses the device’s data to visualize the current health condition of the patient in real time. This enables effective decision making for the health personnel before they even go into the operating room for the daily health inspection.

This device is used for sending data and information to SmartMedic solution’s tablet that in turn sends data to the Stryker cloud storage for further analysis. This device will not allow the user to transfer the patient’s data to any other external or connected system for further processing. The patient data is encrypted and stored locally and on the 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 have a usual good network security and communication tools environment, however Stryker recommends the user to follow the best practiced 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.

## 3.6 Smart Medic Solution’s Component

**SmartMedic Solution Component: Device**

SmartMedic devices consist of the sensors that are used to retrieve the health vital data such as weight, position etc. This device is only used for routing data and information to the SmartMedic solution’s tablet.

**SmartMedic: Tablet**

SmartMedic solution’s tablet that further routes data to the Stryker cloud storage for further analysis. The tablet collects the data from all the SmartMedic devices which are configured to route the data towards the SmartMedic cloud application.

**SmartMedic: Nurse Station Application**

SmartMedic: Nurse Station Application receives an alert for the unexpected change of the health vital, which uses the device’s data to visualize the current health condition of the patient in real time to enable effective decision making for the health personnel before they even go into the operating room for the daily health inspection.

**SmartMedic: Communication Network**

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

# 04 User Account Management

**SmartMedic: Tablet**

***Existing Security Features:***Only Stryker’s service engineer is authorized to manage user account

***Recommendation for customer (HDO):*** No user account management by HDO/hospital staff.

**SmartMedic: Nurse Station Application**

***Existing Security Features:*** HDO/hospital staff is only authorized to manage the user account on the Nurse Station web application. Stryker will provide the personal authentication credentials for the same.

***Recommendation for customer (HDO):*** No user account management by customer. Stryker’s customer can access the Nurse Station web application using the credentials provided by Stryker.

# 05 Access control policy and management

**SmartMedic Solution Component: Device, Tablet** **and Nurse Station Application**

***Existing Security Features:***Only Stryker’s service engineer is authorized to access the SmartMedic solutions component whenever needed, at the time of maintenance. The tablet is placed inside an enclosure. Access to the tablet is only provided to Stryker Service Personnel. Stryker’s customer is only authorized to access the Nurse Station web application. Stryker will provide the personnel with authentication credentials for the same.

***Recommendation for customer (HDO):*** Stryker’s customer can access the Nurse Station web application using the credentials provided by Stryker. The management of physical security aspects of the HDO's IT system, networks and other configuration items is a key responsibility of the HDO's IT network management.

# 06 Security Awareness Training

**SmartMedic Solution Component: Device**, **Tablet and Nurse Station Application**

***Recommendation for customer (HDO):*** Customer aware and train the user . Only Stryker’s service engineer is authorized to access the SmartMedic solutions component device whenever needed, at the time of maintenance. HDO is not allowed to access and manage the device and tablet component.

HDO’s user can access the Nurse Station web application using the credentials provided by -Stryker and can log out of the system whenever the Nurse Station application is not in use.

All network connections are considered in determining appropriate security controls. The HDO IT team will provide a 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 the Stryker cloud.

# 07 Incident Management, Response, Training, Testing, Handling, Monitoring & Reporting

**SmartMedic Solution Component: Device, Tablet and Nurse Station Application**

***Existing Security Features:***Only Stryker’s service engineer is authorized to perform testing and maintenance of the SmartMedic Solution’s component device, whenever needed, at the time of incident response. When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is 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. Malware detection is crucial with malware’s prevalence because it functions as an early warning system for the computer secure regarding cyberattacks. It keeps hackers out of the computer and prevents the information from being compromised. Only Stryker Technical Team is authorized to repair or resolve issues whenever a severe malware is detected.

Vulnerability Management

* Implementation of security scanning tools within the organization
* Onboarding the application/infrastructure to the scanning tool
* Identification 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 needs to update the software or hardware if needed.
* Client needs to test or validate the effectiveness of the 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 needs 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

* Devices functioning training should be provided to staff members utilizing the devices
* Client needs to evaluate the security training requirements for this product and needs to determine that standard user security and awareness training for business purpose to users.
* 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.

***Recommendation for customer (HDO):*** Customer are not allowed to access this component*.* Please reach out to Stryker Customer Care for incident response. Whenever severe malware is detected it is resolved by the service engineer. The customer has to block few IOCs and IOAs in their network devices. The customer is highly recommended to use the network firewall. SmartMedic solution should be behind a stateful firewall. The 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.

# 08 Contingency Plan: Testing, Maintenance and Training

**SmartMedic Solution Component: Device, Tablet, Nurse Station Application and Wireless Network**

***Existing Security Features:***Only Stryker’s service engineer is authorized to perform testing and maintenance of the SmartMedic solutions component device whenever needed at the time of maintenance. When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is 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.

***Recommendation for customer (HDO):*** Contingency planning and management (e.g. restoring a system or a network segment or certain applications) is a key responsibility of the HDO’s IT network management.

If an unfortunate event happens with/without uncertainty then HDO has to respond to such events and maintain the HDO internal document for the same.

# 09 Trustworthiness- CIA Triad & Their Responsibilities

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:*** SmartMedic solution uses a strong, secure communications protocol for communicating among the components. The ability of the SmartMedic solution ensures the confidentiality of transmitted sensitive information and transmits sensitive data only via a point-to-point dedicated channel between SmartMedic device and the Tablet, the Tablet and SmartMedic cloud application & SmartMedic Cloud application and Nurse Station Application.

***Recommendation for customer (HDO):*** Stryker’s customers have to ensure that SmartMedic Device is connected to the tablet and always up & runningand powered, hence, making it available 24x7. All network connections are 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. Stryker Cloud and Nurse Station which will maintain the confidentiality. Stryker customer has to make sure that the SmartMedic Tablet is always connected to the Internet and power. Stryker’s customer can access the Nurse Station web application using the credentials provided by Stryker. Sharing of personal credentials is not advised, in order to maintain confidentiality.

# 10 System Maintenance

**SmartMedic Solution Component: Device and Tablet**

***Existing Security Features:***Only Stryker’s service engineer is authorized to perform testing and maintenance of the SmartMedic solution’s component devices, whenever needed, at the time of maintenance. SmartMedic system maintenance is planned/designed & can be performed based on the component in the SmartMedic environment/platform.

***Recommendation for customer (HDO):*** Customers are not allowed to access SmartMedic device and Tablet component. Please reach out to Stryker Customer Care for system maintenance.

**SmartMedic: Nurse Station Application**

***Existing Security Features:*** When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is 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.

# 11 Configuration settings

***Recommendation for customer (HDO):*** HDOs responsibility - Configuration management is the discipline of ensuring the integrity of HDOs networking IT configuration items (SW, HW, tools, procedures, etc.).

HDO users are allowed to customize the configured logout time.

# 12 System and information integrity

***Recommendation for customer (HDO):*** It is the HDO's responsibility to maintain the integrity for its IT systems. The Nurse Station application can be accessed through web interface on a system which is owned by the HDO. The Tablet is already enclosed and hence tamper proof. Entry to the Tablet is only possible for the Stryker service personnel.

Information systems security relies on the practice of ensuring and maintaining the confidentiality, integrity, and availability of information systems and the data transmitted, processed, and/or stored on those systems. Integrity is defined as guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. It is the assertion that data can only be accessed or modified by authorized entities.

# 13 Malicious code protection

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:*** The Tablet is already enclosed and hence tamper proof. Entry to the Tablet is only possible for the Stryker service personnel. SmartMedic solution uses a strong secure communications protocol for communicating among the components. The ability of the SmartMedic solution ensures the confidentiality of transmitted sensitive information.

***Recommendation for customer (HDO):*** It is the HDO's responsibility to maintain the integrity for its IT systems. The Nurse Station application can be accessed through web interface on a system which is owned by the HDO.

Following these security practices, can help you reduce the risks associated with malicious code:

**Install and maintain antivirus software.** Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up-to-date.

**Use caution with links and attachments.** Take appropriate precautions when using email and web browsers to reduce the risk of an infection. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to come from people you know. (Using Caution with Email Attachments)

**Block pop-up advertisements.** Pop-up blockers disable windows that could potentially contain malicious code. Most browsers have a free feature that can be enabled to block pop-up advertisements.

**Use an account with limited permissions.** When navigating the web, it's a good security practice to use an account with limited permissions. If you do become infected, restricted permissions keep the malicious code from spreading and escalating to an administrative account.

**Disable external media AutoRun and AutoPlay features.** Disabling AutoRun and AutoPlay features prevents external media infected with malicious code from automatically running on your computer.

**Change your passwords.** If you believe your computer is infected, change your passwords. This includes any passwords for websites that may have been cached in your web browser. Create and use strong passwords, making them difficult for attackers to guess. (Choosing and Protecting Passwords and Supplementing Passwords)

**Keep software updated.** Install software patches on your computer so attackers do not take advantage of known vulnerabilities. Consider enabling automatic updates, when available. (Understanding Patches and Software Updates)

**Back up data**. Regularly back up your documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an infection, your information will not be lost.

**Install or enable a firewall**. Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer. Some operating systems include a firewall; if the operating system you are using includes one, enable it. (Understanding Firewalls for Home and Small Office Use)

**Use anti-spyware tools.** Spyware is a common virus source, but you can minimize infections by using a program that identifies and removes spyware. Most antivirus software includes an anti-spyware option; ensure you enable it.

**Monitor accounts.** Look for any unauthorized use of, or unusual activity on your accounts—especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.

**Avoid using public Wi-Fi.** Unsecured public Wi-Fi may allow an attacker to intercept your device’s network traffic and gain access to your personal information.

# 14 Information system monitoring

***Recommendation for customer (HDO):*** It is the HDO's responsibility to maintain the integrity for its IT systems. The Nurse Station application can be accessed through web interface on a system which is owned by the HDO.

* Monitor critical systems and networks for indicators of attacks, and unauthorized connections to critical information systems.
* Assess identified indicators and report unauthorized activity to the Position of Authority and information system owner HDO.
* Ensure the integrity of monitoring tools and the information obtained from those tools.

# 15 Information handling and retention

***Existing Security Features:***Health data is retained in cloud. Retentions policy for the data storage is of 6 months.

# 16 Transmission confidentiality and integrity

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:***Transmits sensitive data only via a point-to-point dedicated channel between SmartMedic device and Tablet. The data at rest and data in motion is 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. SmartMedic solution will handle data integrity checking mechanisms of stored health data. Customer only needs to provide the secure encrypted channel for the communication between the SmartMedic solution’s components i.e. SmartMedic cloud application and the Nurse Station user.

***Recommendation for customer (HDO):*** The customer is not allowed to access device and tablet component*.* The customer only needs to provide the secure encrypted channel for communication between the SmartMedic solution’s component i.e., the tablet and SmartMedic cloud application. All network connections are considered in determining appropriate security controls like Wi-Fi (consider authentication protocols supported, such as WPA2 EAP-TLS) for the communication between the SmartMedic solution’s components i.e., Stryker Cloud and the Nurse Station.

# 17 Security Alerts, Advisories, and Directives

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:*** 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 being compromised. Only Stryker Technical Team is authorized to repair or resolve issues whenever severe malware is detected.

***Recommendation for customer (HDO):*** The customer is not allowed to access this component*.* Please reach out to Stryker Customer Care for security Alert, whenever severe malware is detected and get it resolved by the service engineer. Customer has to block few IOCs and IOAs in their network devices. It is highly recommended that the customer (HDO) should use network firewall. SmartMedic solution should be behind stateful firewall. 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.

Stryker’s customer can access the Nurse Station web application using the credentials provided by Stryker.

# 18 Flaw remediation & Vulnerability Management

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:***When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is 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.

***Recommendation for customer (HDO):*** The customer is not allowed to access this component*.* Any potential security vulnerabilities that the customer may become aware of with regard to the SmartMedic Device must be communicated to Stryker customer care and the same will be handled through the post market complaints management process for assessment and required actions including any updates needed for the customers.

Stryker’s customer can access the Nurse Station web application using the credentials provided by Stryker.

# 19 Cyber Security Product Upgrades

**SmartMedic Solution Component: Device and Tablet**

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

***Recommendation for customer (HDO):*** The customer is not allowed to access this component*.*

# 20 Security Program Integration

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:***Stryker will take care of the security program integration, scanning, security testing, and vulnerability management of SmartMedic solution for this component.

***Recommendation for customer (HDO):*** The customer is not allowed to access this component*.* Please reach out to Stryker Customer Care for security program integration.

# 21 Secure Decommissioning

**SmartMedic Solution Component: Device and Tablet**

***Recommendation for customer (HDO):*** Please reach out to Stryker Customer Care for secured decommissioning*.*

# 22 Cryptographic Protection & Management

**SmartMedic Solution Component: Device, Tablet and Nurse Station Application**

***Existing Security Features:***The data at rest is 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. SmartMedic solution will handle data integrity checking mechanisms of stored health data. The customer only needs to provide the secure encrypted channel for the communication between the SmartMedic solution’s component i.e., the Device & Tablet, the Tablet & SmartMedic Cloud Application, SmartMedic Cloud Application and the Nurse Station Application.

***Recommended for the Stryker’s customers:*** The customer is not allowed to access SmartMedic Device and Tablet component*.* All network connections are considered in determining appropriate security controls. The HDO 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 ablet and Stryker cloud

# 23 Malware Detection/Protection

**SmartMedic: Tablet**

***Existing Security Features:***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 being compromised. Only Stryker Technical Team is authorized to repair or resolve issues whenever severe malware is detected.

***Recommendation for customer (HDO):*** Customer is not allowed to access this component*.* Whenever severe malware is detected get it resolved by the service engineer. Customer has to block few IOCs and IOAs in their network devices. It is highly recommended that the customer (HDO) should use network firewall. SmartMedic solution should be behind stateful firewall. The 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.

**SmartMedic: Communication Network:**

***Recommendation for customer (HDO):*** Whenever severe malware has been detected it is resolved by the service engineer. Customer has to block few IOCs and IOAs in their network devices. It is highly recommended that the customer (HDO) should use network firewall. SmartMedic solution should be behind stateful firewall. The 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.

# 24 Roadmap for Third Party Components in Device Life Cycle

**SmartMedic Solution Component: Device and Tablet**

***Existing Security Features:***Stryker has evaluated third -party components as per the requirement identified and adequate actions have been implemented in the application. Stryker will be evaluating high-risk third-party components periodically and communicate to customers for any updates required during the product lifecycle.

***Recommendation for customer (HDO):*** Customer is not allowed to access this component*.*

# 25 Health Data Storage Confidentiality

**SmartMedic: Tablet and Nurse Station Application**

***Existing Security Features:***The data at rest is 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.

***Recommendation for customer (HDO):*** The customer only needs to provide the secure encrypted channel for the communication between the SmartMedic solution’s component i.e. the tablet and SmartMedic cloud application. It is advised that personal credentials should not be shared with anyone.

# 26 System and Application Hardening

**SmartMedic Solution Component: Device, Tablet & Nurse Station Application**

***Existing Security Features:***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 issues. System hardening is a collection of tools, techniques, and best practices to reduce vulnerability in the application, systems, and other areas. SmartMedic solution uses the strong secure communications protocol for communicating among the components. The ability of the SmartMedic solution ensures the confidentiality of transmitted sensitive information. It transmits sensitive data only via a point-to-point dedicated channel between SmartMedic Device and Tablet.

***Recommendation for customer (HDO):*** The customer is not allowed to access SmartMedic device*. The c*ustomer is aware and trains the user that all network connections are 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, 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.

Stryker’s customer can access the Nurse Station web application using the credentials provided by Stryker. It is advised that personal credentials should not be shared with anyone.

# 27 Physical Locks

***Recommendation for customer (HDO):*** The Tablet is placed inside an enclosure. Access to the Tablet is only provided to Stryker Service Personnel. The management of physical security aspects of the HDO's IT system, networks and other configuration items is a key responsibility of the HDO's IT network management.

***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*