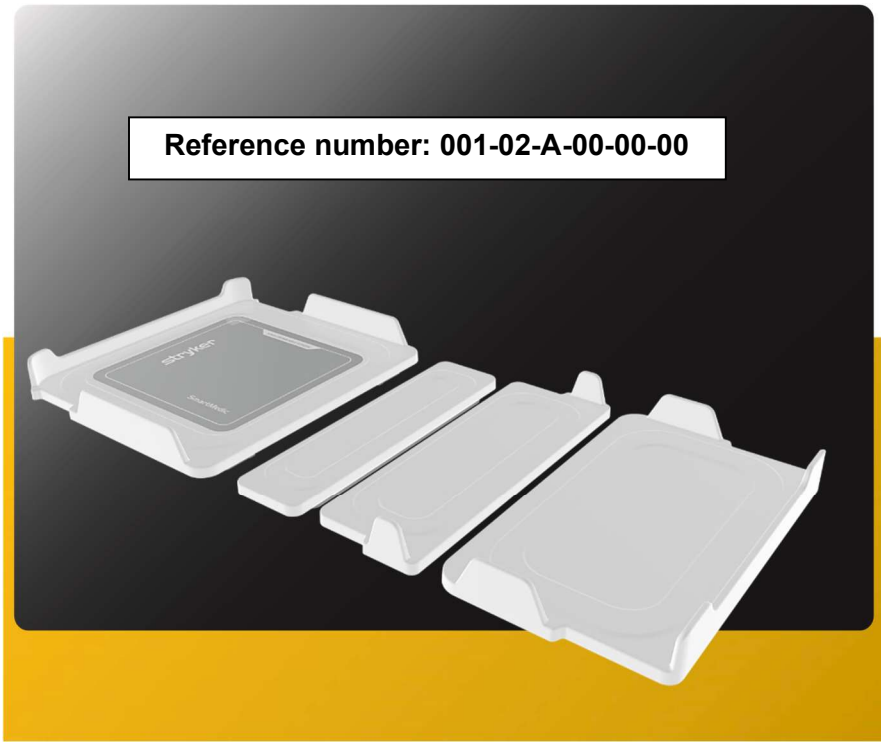
SmartMedic

Security Operations Manual



This page intentionally left blank

stryker

Table of Contents

01 PURPOSE 5
02 DEFINITIONS 5
03 PRODUCT DESCRIPTION 7
3.1 Device and Manufacturer Identification 7
3.2 Device Intended Use 8
3.3 Vulnerability Intake and Monitoring 9
3.4 System Characterization and System Assets 9
3.5 System Security Context and Intended Environment 9
3.6 SmartMedic Solution Components 10
04 MANAGEMENT OF PII and PHI 11
05 AUTOMATIC LOGOFF 11
06 AUDIT CONTROLS 11
07 AUTHORIZATION 11
7.1 Access control policy and management 11
08 CYBER SECURITY PRODUCT UPGRADES 11
8.1 System Maintenance 12
09 HEALTH DATA DE-IDENTIFICATION 12
10 DATA BACKUP AND DISASTER RECOVERY 12
10.1 Contingency Plan: Testing, Maintenance and Training 12
10.2 Configuration settings 12
11 EMERGENCY ACCESS 13
12 HEALTH DATA INTEGRITY AND AUTHENTICITY 13
13 MALWARE DETECTION/PROTECTION 13
13.1 Flaw remediation & Vulnerability Management 13
13.2 Malicious code protection 14
13.3 Information system monitoring 15
13.4 Security Alerts, Advisories, and Directives 15
14 NODE AUTHENTICATION 15
15 CONNECTIVITY CAPABILITIES 15
16 PERSON AUTHENTICATION 16
16.1 User Account Management 16
16.2 Cryptographic Protection & Management 16
17 PHYSICAL LOCKS 16
18 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE 16
19 SOFTWARE BILL OF MATERIALS 17
20 SYSTEM AND APPLICATION HARDENING 17
21 HEALTH DATA STORAGE CONFIDENTIALITY 17
22 TRANSMISSION CONFIDENTIALITY 17
23 TRANSMISSION INTEGRITY 18
23.1 System and information integrity 18
23.2 Trustworthiness- CIA Triad & Their Responsibilities 18
23.3 Information handling and retention 18
24 REMOTE SERVICE 18
25 SECURITY PROGRAM INTEGRATION 18

25.1 Incident Management, Response, Training, Testing, Handling, Monitoring & Reporting 19
25.2 Security Awareness Training 20
26 SECURE DECOMMISSIONING 20
27 Appendix I: Smart Medic Third Party Licensing Terms and Attributions)…… .....I to XIII

01 PURPOSE

This Security Operations Manual (SOM) details different security features & configurations incorporated with the SmartMedic solution.

It also provides the security guidelines for the customer to be aware during the device operation.

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.

IOA – Indicators of attack

An IOA represents a series of actions that an adversary must conduct to succeed.

IOC – Indicator of compromise

Indicator of compromise or IOC is a forensic term that refers to the evidence on a device that points out to a security breach.

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

Entity with legal authority to design, manufacture, package and label the product or device before it is placed on the market.

Medical Device

Any instrument, apparatus, software, material, or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for diagnosis, monitoring, treatment, alleviation of or compensation for an injury.

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

Refer 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).

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.

User

Refer Operator.

03 PRODUCT DESCRIPTION

SmartMedic is an AC Powered (with AC to DC adaptor) device intended for use on Hospital Beds. It is designed to provide improved patient care in the hospital facility. The device is secured in place on top of the bed frame and under the bed's mattress. The device can provide patient weight, turn indication and share information with authorized hospital nurse station. The system shares and displays information on hospital's Nurse station through cloud application. The device also supports functionality for placing x-ray cassette without moving the patient on bed.

Manufacturer Name	Stryker
Stryker Division	Stryker Global Technology Center Private Limited
Address	Stryker Global Technology Center Private Limited, International Tech Park Gurgaon, 5th floor, Block I, Sector 59, Behrampur, Gurgaon-122101, India
Device Description	SmartMedic is an AC Powered (with AC to DC adaptor) device intended for use on Hospital Beds. It is designed to provide improved patient care in the hospital facility. The device is secured in place on top of the bed frame and under the bed's mattress. The device can provide patient weight, turn indication and share information with authorized hospital nurse station. The system shares and displays information on hospital's Nurse station through cloud application. The device also supports functionality for placing x-ray cassette without moving the patient on bed.
Device Model	**SmartMedic 001-02-A-00-00-00**
Manufacturer Contact Information	**Manufactured at**: Plot No. 130, 4th Phase KIADB Industrial Area Bommasandra-Jigani Link Road, Bangalore, Karnataka 560099, India **Marketed and Distributed by:** Stryker India Pvt.Ltd. India Customer care No.: 1800-103-8030 Email Id: service.india@stryker.com

Table 1.1 Product Description

3.1 Device and Manufacturer Identification

Device

SmartMedic

Manufacturer

Stryker Global Technology Center Private Limited,
International Tech Park Gurgaon,
5th floor, Block I, Sector 59,
Behrampur, Gurgaon-122101, India

3.2 Device Intended Use

Device name (unique identifier)	SmartMedic (Part Number - 001-02-A-00-00-00)
Intended medical indication	SmartMedic is intended to be used as an accessory to hospital Medical Bed for measuring patient's weight and alert caregiver to turn patient. The device is intended to take patient's weight on medical bed in flat position. The device is intended to take weight of adult patients. Device is intended to provide relative change in patient's weight. For pediatric patients, the device is intended to provide weight and relative changes in weight. The device intends to give patient turn notification for the adult patient only. Device is intended to be used in Indian hospital environment. The device is intended to help caregiver to place x-ray cassette without moving the patient. It is also not intended for patients having height less than 4.0 ft or more than 6.0 ft, and weight less than 10Kg or more than 135Kg. Device is not intended for using Patient turn feature with Pediatric Patients. The maximum safe working load (including patient, mattress, sheets, pillows, and accessories) for SmartMedic is 155kg. SmartMedic is not intended to be used for infants.
Intended patient population (including population at greatest risk)	SmartMedic to provide weight for all age groups from Pediatric to adult population.
Intended part of the body or type of tissue applied to or interacted with	Mattress (Applied part Type B)
Intended user profile	Nurse, Intensivist / Doctors
Intended condition of use (including Expected Life)	Intended to be used in Indian Hospital environment (Temp. 15°C - 30°C) Expected service life: 4 years.

Intended use as per reference DIOV document D001020006
Refer IFU (Instructions for use) document 001-02-L-13-00-00 for more details

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 on the assessment report, Stryker determines if further actions similar to providing security updates and/or providing information to the customer in targeted time. 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 (contact details: refer to the backside of the manual) and the same will be handled through the post market complaints management process to do the assessment and take required actions including updates/patches for the customers.

3.4 System Characterization and System Assets

SmartMedic solution is comprised of

1. SmartMedic Device
   SmartMedic device calculates the data such as weight & position with the help of sensors.
2. SmartMedic Tablet
   SmartMedic tablet is responsible to route the data to the Stryker cloud storage for further analysis.
3. SmartMedic Nurse Station Application
   The Nurse Station Application will be used to monitor the weight, position data, and trend of weight and position change on SmartMedic devices.
4. Secure Communication Network
   Communication network is used to transmit the information from hospital's environment to cloud.

3.5 System Security Context and Intended Environment

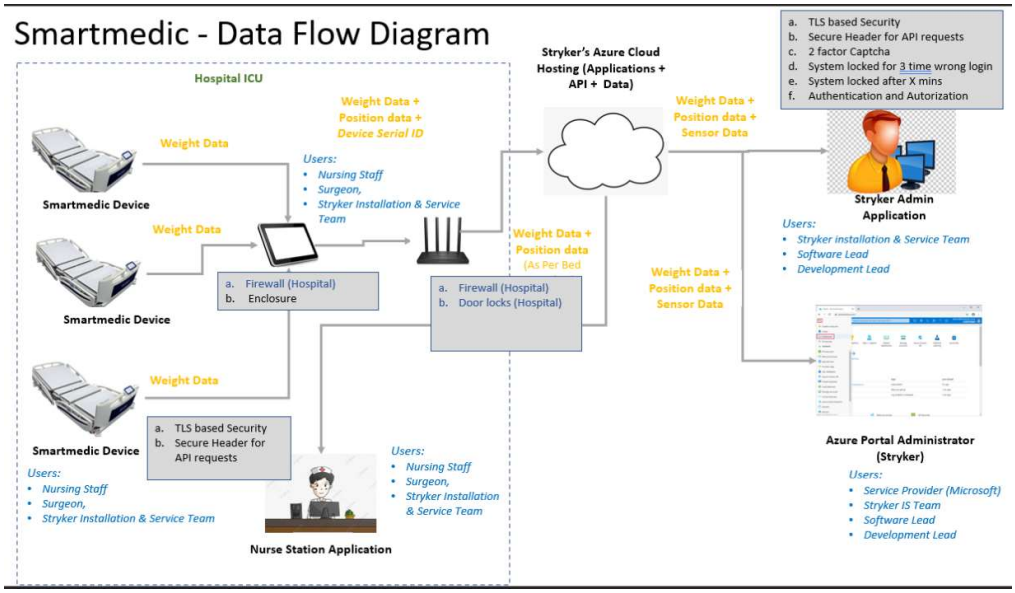


Figure 1: System Security

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.
- Access control measures to ensure only authenticated and authorized personnel are allowed access to network elements, stored information, services, and applications.
- Communication between SmartMedic tablet and device should be in the secure channel interface.
- General patch management practices that ensure timely security patch updates.
- Use the good network security and communication tools.
- Security awareness training.

3.6 SmartMedic Solution Components

SmartMedic Solution Components: Device

SmartMedic device measures the data such as weight & position with the help of sensors. This device is also responsible to route the data to SmartMedic tablet after the measurement.

SmartMedic: Tablet

SmartMedic tablet is responsible in collecting the data from all the configured SmartMedic devices and routing it to the Stryker cloud storage.

SmartMedic: Nurse Station Application

SmartMedic: Nurse Station Application receives the data and helps to monitor weight, weight trend and patient turn.

Nurse Station application will be used to monitor the weight, position data, and trend in default flow.

Admin Application shall be used to create/manage hospitals and ICUs for the nurse station application. The admin application facilitates user to view linked SmartMedic devices to the bed in the hospital with connection status and software upgrade status. The admin panel offers an effective solution to upgrade the software of the SmartMedic devices.

SmartMedic: Communication Network

SmartMedic: Communication network is used to transmit the information from hospital's environment to cloud.

04 MANAGEMENT OF PII and PHI

SmartMedic Solution Components (Device, Tablet, Nurse Station Application and SmartMedic app (Stryker Admin Web Application)) doesn't display, transmits, stores, or modifies Personally Identifiable Information (PII, e.g., electronic Protected Health Information (ePHI)).

Patient details are anonymized and mapped to patient id. Using the patient id, personal details can't be retrieved. The data at rest is encrypted using a strong encryption mechanism implemented within the SmartMedic solution, which safeguards the data from unauthorized access.

05 AUTOMATIC LOGOFF

SmartMedic Solution Components: SmartMedic app (Stryker Admin Web Application) and Nurse Station Application

The Stryker Admin Web Application shall allow the user to be logged out if the session has ended or after 8 minutes of inactivity.
Configurable time out is provided for the Nurse Station Application.

06 AUDIT CONTROLS

SmartMedic Solution Components: SmartMedic app (Stryker Admin Web Application)

Invalid login credentials (email or password) event is audited, only 3 attempts provided for validation.

07 AUTHORIZATION

7.1 Access control policy and management

SmartMedic Solution Components: Device, Tablet and Nurse Station Application

Existing Security Features: Only Stryker's service engineer has authorization to access the SmartMedic solution components (device, tablet) 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 provides 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.

08 CYBER SECURITY PRODUCT UPGRADES

SmartMedic Solution Components: Device and Tablet

Existing Security Features: The SmartMedic platform components does not have any updates installation policy implemented. Hence, the users doesn't get any notification of 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): Any information regarding cyber security product upgrades can be requested from Stryker.

8.1 System Maintenance

SmartMedic Solution Components: Device and Tablet

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

Recommendation for customer (HDO): The required access and corresponding maintenance of the device and tablet is not provided for HDO. 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.

09 HEALTH DATA DE-IDENTIFICATION

SmartMedic solution components doesn't collect/store/process any kind of PII/PHI data. Hence health data de-identification is not considered for SmartMedic solution components.

10 DATA BACKUP AND DISASTER RECOVERY

10.1 Contingency Plan: Testing, Maintenance and Training

SmartMedic Solution Components: 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 solution components (device, tablet) on need basis, maybe at the time of incident reported. When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability's exploitability and impact is conducted. Based on the assessment report, Stryker determines if further actions similar to providing security updates and/or providing information to the customer in targeted time. 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.

10.2 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.).

Only Stryker's service engineer has authorization to access the SmartMedic solution components (device, tablet) whenever needed to change the configuration settings.

HDO users are allowed to customize the following:

- Wireless Access Point (Wi-Fi AP).

11 EMERGENCY ACCESS

SmartMedic solution components doesn't contain the personally identifiable information. Hence no option for the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.

12 HEALTH DATA INTEGRITY AND AUTHENTICITY

SmartMedic solution components doesn't have any stored data on the device and other components.

SmartMedic solution components doesn't contain the personally identifiable information. Hence no option for the device user to access personally identifiable information.

13 MALWARE DETECTION/PROTECTION

SmartMedic: Tablet

Existing Security Features: The standalone SmartMedic tablet by default contains malware detection functionality, as the malware detection is crucial as attackers exploiting the system in multiple ways and hence it can serve as an early warning to the system regarding cyberattacks. Only Stryker Technical Team is authorized to repair or resolve issues whenever severe malware is reported.

Recommendation for customer (HDO): Customer (HDO) needs to provide the malware protection for NSA system.

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.

13.1 Flaw remediation & Vulnerability Management

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: Stryker had performed the system and application security testing along with secure code review of SmartMedic platform components. When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability's exploitability and impact is conducted. Based on the assessment report, Stryker determines if further actions similar to providing security updates and/or providing information to the customer in targeted time. Vulnerability information may also be requested from Stryker at any time.

Recommendation for customer (HDO): Any potential security vulnerabilities that the customer may become aware of with regard to the SmartMedic platform components 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.

13.2 Malicious code protection

Malicious code is harmful computer programming scripts designed to create or exploit system vulnerabilities. This code is designed by an attacker to cause unwanted changes, damage, or ongoing access to computer systems.

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: The Tablet is already enclosed and hence tamper proof. Access (physical/operational) 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 secure design of the SmartMedic solution ensures the confidentiality of transmitted 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 a HDO to reduce the risks associated with malicious code:

Install and maintain antivirus software. Antivirus software recognizes malware and protects the Nurse station hosting system. 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 virus attacks. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to come from people, you are aware of. (Using Caution with Email Attachments)

Block pop-up advertisements. Pop-up blockers disable browser 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 the system got affected with virus, 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 the system.

Change your passwords. If you believe the system is infected, change the passwords. This includes any passwords for websites that may have been cached in the 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 the system 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 the documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an attack, then information won't be lost.

Install or enable a firewall. Firewalls can prevent some types of attacks by blocking malicious traffic before it enters the system. Some operating systems include a firewall; if the operating system you are using includes one, enable it.

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

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

13.3 Information system monitoring

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.

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 (IOA), 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.

13.4 Security Alerts, Advisories, and Directives

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: No runtime alerts configured for SM platform.

Stryker can be alerted for the following:

- Any suspected/confirmed malware found on the system
- Any unexpected system behavior observed
- Any suspected misuse of the device (can confirm through logs)
- Incorporated methods detect that any data inappropriately accessed or copied from the device
- From the report of forensic inspection of the device

For any reported vulnerability in the product, the Stryker follows the practice of issuing security advisory along with the corresponding directives.

Recommendation for customer (HDO): Any potential security vulnerabilities that the customer may become aware of with regard to the SmartMedic platform components 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.

14 NODE AUTHENTICATION

Only Stryker made/ authenticated devices should be able to communicate with SmartMedic device and tablet.
Bluetooth Authentication on device, Device ID act as the key for device authentication.
Tablet provisioning on IOT Hub with tokens (Applicable to SmartMedic device, Tablet and Cloud connections).

15 CONNECTIVITY CAPABILITIES

HDO users are allowed to customize the following:

- Wireless Access Point (Wi-Fi AP).

All SmartMedic solution components (Device, Tablet & Nurse Station Application) use the HDO's wi-fi AP for communication.

16 PERSON AUTHENTICATION

16.1 User Account Management

SmartMedic: Tablet

Existing Security Features: Only Stryker's service engineer has a user account and been provided with the authorization to access.

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

SmartMedic: Nurse Station Application

Existing Security Features: HDO/hospital staff has a user account and been provided with the authorization to access. Stryker provides the unique authentication credentials for the same.

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

16.2 Cryptographic Protection & Management

SmartMedic Solution Components: Device, Tablet and Nurse Station Application

Existing Security Features: Stryker owned SmartMedic components such as (SmartMedic device, tablet) & HDO components (NSA system, Wi-Fi Access Point) employ cryptographic protection. SmartMedic device & tablet are designed such that Stryker made/authenticated (HDO) can only establish communication with them. Sensitive data, such as crypto elements (keys, tokens, certificates) are secured with cryptographic protection. HDO Wi-Fi access point, used in secure communication channel protected along with secured authentication credentials. Hence, communication between the SmartMedic solution components i.e., the Device & Tablet, the Tablet & Stryker Cloud, Stryker Cloud & the Nurse Station Application can be cryptographically protected.

Recommended for the Stryker's customers: All HDO network connections should be considered in determining appropriate security controls. The HDO has to provide the secure encrypted channel for the communication between the SmartMedic solution components i.e., the tablet and Stryker cloud.

Any information regarding cryptographic protection can be requested from Stryker.

17 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.

18 ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE

SmartMedic Solution Components: 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 complete SmartMedic platform. 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): Any information regarding Roadmap for Third Party Components in Device Life Cycle can be requested from Stryker.

19 SOFTWARE BILL OF MATERIALS

It is addressed in the Software Development Plan prepared by Stryker.

20 SYSTEM AND APPLICATION HARDENING

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: Stryker had performed the system and application security testing along with secure code review of SmartMedic platform components. The testing report has been evaluated to identify the exploited vulnerabilities & provided the secure interfaces. The SmartMedic device (tablet) has been hardened to operate in Kiosk mode and preconfigured with anti-malware to identify run time vulnerabilities. It transmits encrypted data only via a point-to-point dedicated secure channel between SmartMedic Device and Tablet. The secure design of the SmartMedic solution ensures the confidentiality of transmitted information.

Recommendation for customer (HDO): Customer (HDOs) responsibility to be aware and train the appropriate user. The customer will provide the secure encrypted channel for the communication between the SmartMedic solution 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 unique id provided by Stryker. It is advised that authentication credentials should not be shared with anyone who is not HDO related.

21 HEALTH DATA STORAGE CONFIDENTIALITY

SmartMedic: Tablet and Nurse Station Application

Existing Security Features: SmartMedic platform has weight & position considered as data. Patient details are anonymized and mapped to patient id. Using the patient id, personal details can't be retrieved. The data at rest is encrypted using a strong encryption mechanism implemented within the SmartMedic solution, which safeguards the data from unauthorized access.

Recommendation for customer (HDO): The customer only needs to provide the secure encrypted channel for the communication between the SmartMedic solution components i.e., the tablet and Stryker cloud. It is advised that the related credentials should not be shared with anyone.

22 TRANSMISSION CONFIDENTIALITY

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: SmartMedic solution platform transmits data only via a point-to-point dedicated channel between SmartMedic device and Tablet. The data at rest and data in transit is encrypted using a strong encryption mechanism implemented within the SmartMedic solution, which safeguards the data from unauthorized access. SmartMedic solution will handle data integrity checking mechanisms of transmitted data. Customer (HDO) only needs to provide the secure interface for the communication between the SmartMedic solution components i.e., Stryker cloud and the Nurse Station application.

Recommendation for customer (HDO): The access and management of the device and tablet is not provided for HDO. The customer (HDO) needs to provide the secure interface for communication between the SmartMedic solution component i.e., the tablet and Stryker cloud. All network connections are considered in determining appropriate security controls. The HDO IT team will provide a secure encrypted channel for the communication between the SmartMedic solution components i.e., Stryker Cloud and the Nurse Station Application.

23 TRANSMISSION INTEGRITY

23.1 System and information integrity

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.

Recommendation for customer (HDO): It is the HDO's responsibility to maintain the integrity for its IT systems.

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

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. Access (physical/system) to the Tablet is only possible for the Stryker service personnel.

23.2 Trustworthiness- CIA Triad & Their Responsibilities

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: SmartMedic solution uses a strong, secure communications protocol for reliable/safe communication among the components. The secure design of the SmartMedic solution ensures the Confidentiality, Integrity & Availability of transmitted information and transmits data only via a point-to-point dedicated channel between SmartMedic device and Tablet, Tablet and Stryker cloud, Stryker cloud and Nurse Station Application.

Recommendation for customer (HDO): Stryker customer (HDO) have to ensure that SmartMedic Device is connected to the tablet and always accessible. Hence, making it available 24x7. All network connections are considered in determining appropriate security controls. The customer will provide the secure encrypted channel for the communication between the SmartMedic solution 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 unique id provided by Stryker. Sharing of the related credentials is not advised, in order to maintain confidentiality.

23.3 Information handling and retention

Existing Security Features: All the data transferred from the SmartMedic device to cloud using the tablet. Accumulated data is retained in cloud. Retention policy for the data storage is of 6 months.

24 REMOTE SERVICE

SmartMedic solution components doesn't have remote service provided. All kinds of device maintenance activities performed by a service person via local.

25 SECURITY PROGRAM INTEGRATION

SmartMedic Solution Components: Device, Tablet & Nurse Station Application

Existing Security Features: Stryker will take care of the security program integration, design & code validation, security testing, and vulnerability management of SmartMedic platform.

In addition to this,

1. Stryker has established QMS procedures and trainings for security and safety to be considered during the design & development and post market surveillance of any software driven Medical Device from Stryker. These procedures include the specification of roles & responsibilities.

2. Product security planning: The PSSA, the security architecture and the PS risk analysis define product specific security controls which shall be implemented in the SmartMedic platform and to be considered in accompanying material (e.g., service manual).

3. Customer specific provisions: The SOM establishes application specific security controls and guidance to be considered by the HDO for the security program planning purposes.

Recommendation for customer (HDO): Any information regarding Security Program Integration can be requested from Stryker.

25.1 Incident Management, Response, Training, Testing, Handling, Monitoring & Reporting

SmartMedic Solution Components: Device, Tablet and Nurse Station Application

Existing Security Features: Only Stryker's service engineer is authorized to visit & perform maintenance of the SmartMedic solution components (device, tablet) on need basis, maybe at the time of incident reported. When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability's exploitability and impact is conducted. Based on the assessment report, Stryker determines if further actions similar to providing security updates and/or providing information to the customer in targeted time. Vulnerability information may also be requested from Stryker at any time. Malware detection is crucial as attackers can exploit the system in multiple ways and hence it can serve as an early warning regarding cyberattacks. Only Stryker Technical Team is authorized to repair or resolve issues whenever a severe malware is detected.

Vulnerability Management Process/Practice(s) usually followed includes:

- Usage of Vulnerability/Malware scanning tools
- Onboarding the application/infrastructure to the scanning tool
- Identification and prioritization of the vulnerability as per vulnerability rating such as Critical, High, Medium, and Low
- Planning the vulnerability remediation/mitigation steps
- Integration of the solution and revalidation of the reported vulnerability

For following observations Incident Reporting & Recovery can be initiated:

- Any suspected/confirmed malware found on the system
- Any unexpected system behavior observed
- Any suspected misuse of the device (can confirm through logs)
- Incorporated methods detect that any data inappropriately accessed or copied from the device
- From the report of forensic inspection of the device
- Chances for recovery of data from a damaged or non-functional system

Guidelines to the customer (HDO):

Customer (HDO) is recommended to be up to date with the software being used or latest hardware

- Customer (HDO) needs to test or validate the effectiveness of the system functionality from security perspective at regular intervals
- Functional testing should be performed to identify the weaknesses/vulnerabilities that can be exploited

Risk Management:

- Customer (HDO) needs to conduct security risk identification process which monitors the ongoing security posture of this device/infrastructure and reports any security incidents that might arise.

- Risk assessment should be conducted within the organization to identify the gaps and plan improvements

Training and Awareness:

- Staff members utilizing the devices should be provided with proper training including their functionality
- Customer (HDO) needs to evaluate the security training requirements for this product and also identify any standard user security awareness training needed to users from business perspective.
- 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 that address any issues/concerns related to its use.

Recommendation for customer (HDO): Customer's role is limited to incident reporting & not responsible for the remediation. Please reach out to Stryker Customer Care for incident response. Whenever severe malware is detected, it is resolved by the Stryker 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 configured and used, it can lead to protected and reliable accessibility. It can help in prevention of unauthorized access and network connections that can lead to external threats, IP spoofing & routing attacks and malicious packets.

25.2 Security Awareness Training

SmartMedic Solution Components: Device, Tablet and Nurse Station Application

Recommendation for customer (HDO): It is the customer's (HDO) responsibility to be aware of the product and train the appropriate user(s).

Training for the HDO's user to access the Nurse Station web application using the credentials provided by Stryker and log in/out of the system whenever the Nurse Station application is not in use.

26 SECURE DECOMMISSIONING

SmartMedic Solution Components: Device and Tablet

Recommendation for customer (HDO): Please reach out to Stryker Customer Care for secured decommissioning of Stryker owned SmartMedic components such as (SmartMedic device, tablet). Components owned by HDO should follow the HDO IT policies for secure decommissioning.

Stryker Global Technology Center Private Limited,
International Tech Park Gurgaon,
5th floor, Block I, Sector 59,
Behrampur, Gurgaon-122101, India

Manufactured at:
Plot No. 130, 4th Phase KIADB Industrial Area
Bommasandra-Jigani Link Road, Bangalore, Karnataka 560 099, India

Marketed and Distributed by:
Stryker India Pvt.Ltd. India
Customer care No.: **1800-103-8030**
Email Id: service.india@stryker.com