**[Kneebalancer]**

**Security Operations Manual**

**[Insert device image (optional)]**

**Applies to [Enter relevant part number and version for the product and its software, as applicable]**

This document was prepared by [**department/role name**] of Stryker’s [**division name**] division. See section 3.1 below for contact information.

**Table of Contents**

[1. PURPOSE 4](#_Toc112949888)

[2. DEFINITIONS 4](#_Toc112949889)

[3. PRODUCT DESCRIPTION 6](#_Toc112949890)

[3.1 Product and Manufacturer Identification 6](#_Toc112949891)

[3.2 Product Intended Use 6](#_Toc112949892)

[3.3 Related Manufacturer Programs 6](#_Toc112949893)

[3.4 System Characterization and System Assets 7](#_Toc112949894)

[3.5 System Security Context and Intended Environment 7](#_Toc112949895)

[3.6 Network, Data Flow Diagram 8](#_Toc112949896)

[4. MANAGEMENT OF PII and PHI 8](#_Toc112949897)

[5. AUTOMATIC LOGOFF 9](#_Toc112949898)

[6. AUDIT CONTROLS 9](#_Toc112949899)

[7. AUTHORIZATION 9](#_Toc112949900)

[8. CYBER SECURITY PRODUCT UPGRADES 9](#_Toc112949901)

[9. HEALTH DATA DE-IDENTIFICATION 10](#_Toc112949902)

[10. DATA BACKUP AND DISASTER RECOVERY 10](#_Toc112949903)

[11. EMERGENCY ACCESS 10](#_Toc112949904)

[12. HEALTH DATA INTEGRITY AND AUTHENTICITY 10](#_Toc112949905)

[13. MALWARE DETECTION/PROTECTION 10](#_Toc112949906)

[14. NODE AUTHENTICATION 10](#_Toc112949907)

[15. CONNECTIVITY CAPABILITIES 11](#_Toc112949908)

[15.1 Communication Provisions 11](#_Toc112949909)

[16. PERSON AUTHENTICATION 11](#_Toc112949910)

[17. PHYSICAL LOCKS 11](#_Toc112949911)

[18. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE 11](#_Toc112949912)

[19. SOFTWARE BILL OF MATERIALS 11](#_Toc112949913)

[20. SYSTEM AND APPLICATION HARDENING 11](#_Toc112949914)

[21. HEALTH DATA STORAGE CONFIDENTIALITY 12](#_Toc112949915)

[22. TRANSMISSION CONFIDENTIALITY 12](#_Toc112949916)

[23. TRANSMISSION INTEGRITY 12](#_Toc112949917)

[24. REMOTE SERVICE 12](#_Toc112949918)

[25. SECURITY PROGRAM INTEGRATION 12](#_Toc112949919)

[25.1 Vulnerability Management 12](#_Toc112949920)

[25.2 Incident Response 12](#_Toc112949921)

[25.3 Security Testing 13](#_Toc112949922)

[25.4 Scanning 14](#_Toc112949923)

[25.5 Risk Management 14](#_Toc112949924)

[25.6 Training and Awareness 14](#_Toc112949925)

[26. SECURE DECOMMISSIONING 14](#_Toc112949926)

[27. Appendix 15](#_Toc112949927)

[27.1 List of 3rd party components: 15](#_Toc112949928)

# PURPOSE

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

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

# DEFINITIONS

**API – Application Programming Interface**: An interface for computing that defines interactions between multiple software intermediaries.

**Stryker’s Cloud:** Stryker’s cloud is used for archiving the logs and finished case data to the Azure blob storage with the consent once the internet is available.

**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.

**iOS:** iOS (formerly iPhone OS) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that powers many of the company's mobile devices, including the iPhone.

**Malware:** Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's computer security and privacy.

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

**MPS User- Mako Product Specialist User:** MPS is the user of the Knee balancer application on behalf of surgeon. Creates initial planning and inputs the planning values to Knee Balancer application to generate gap solution. Based on the discussion with surgeon, MPS updates the values in the Mako system.

**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 MPS User.

**PHI - Protected Health Information**: Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media; or transmitted, or maintained, in any other form or medium (source: extracted from 45 CFR Section 160). Note: This is a subset of PII.

**PII - Personally Identifiable Information**: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual ‘s identity… and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (source: from NIST SP 800-122).

**Product:** Refer-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.

**User**: Refer-Operator.

**Vulnerability:** A vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for lurking cybercrimes and are open to exploitation through the points of vulnerability.

# PRODUCT DESCRIPTION

|  |  |
| --- | --- |
| **Manufacturer Name** | **Stryker** |
| **Stryker Division** | Stryker Global Technology Center Private Limited |
| **Address** | Stryker Global Technology Center Private Limited,  Vatika Business Park, 10th Floor, Block two,  Sohna-Gurgaon Rd, Sector 49, Gurugram  Haryana 122002, India |
| **Product Description** | The Knee Balancer application is intended to improve the efficiency that is involved with calculating the implant movements required during TKA intra-operative balancing. The app is a clinical decision support software tool which provides on demand, an automated intra operative plan to the Orthopaedic surgeon based on pre-operative data, captured soft tissue information and surgeon preferences. |
| **Product Version** | 1.0.0 |
| **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](mailto:service.india@stryker.com) |

# Product and Manufacturer Identification

# Product Intended Use

MPS is the user of the Kneebalancer application on behalf of surgeon. Creates initial planning and inputs the planning values to Knee Balancer application to generate gap solution. Based on the discussion with surgeon.

# Related Manufacturer Programs

When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is conducted. Based upon this assessment Stryker determines if further actions are required like providing security updates and/or providing communication to the MPS MPS users in a timely manner. Vulnerability information may also be requested from Stryker at any time.

# System Characterization and System Assets

Kneebalancer solution is comprised of:

1. **Mobile Application**: The application is a clinical decision support software tool which provides on demand, an automated intra operative plan to the Orthopaedic surgeon based on pre-operative data, captured soft tissue information and surgeon preferences.
2. **Stryker’s cloud:** Stryker’s cloud is used for archiving the logs and finished case data to the Azure blob storage with the consent once the internet is available.

# System Security Context and Intended Environment

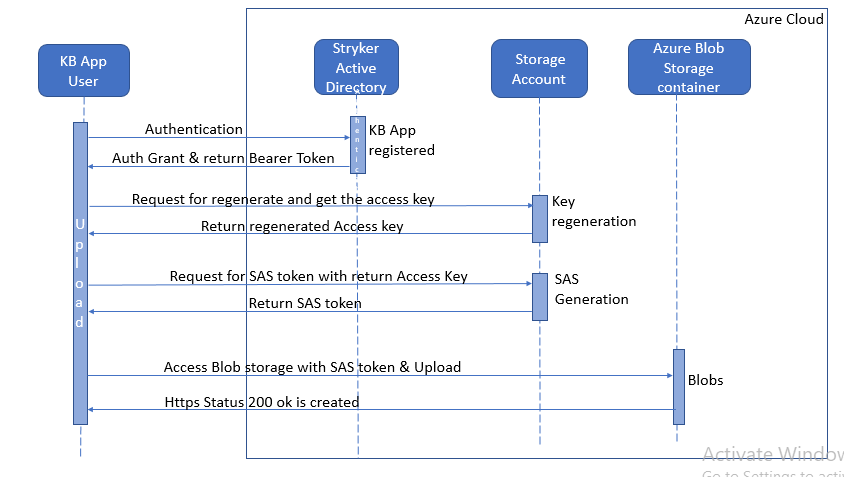


There is no specific requirement for the Kneebalancer application to be fully functional out of usual iOS environment. The application is designed to work completely within iOS device boundary. However, Stryker recommends the MPS user to follow some of the best security standards in order to run the application in a safe and secure environment as follows.

* MPS user login credentials should be secured. Use complex password for the user account as per Stryker policies.
* Do not install unnecessary applications in iOS device. Avoid any third-party application installation.
* Do not click on any suspicious links, documents while using the device.
* Timely update of the operating system and Kneebalancer application to prevent danger of using vulnerable software/OS.
* Security awareness training.

# Network, Data Flow Diagram

High level data flow diagram.



# MANAGEMENT OF PII and PHI

Kneebalancer application does not collect or store any PII or PHI. Thus, no Patient Identification or Patient Health Information is created/stored/processed in the device.

**Management of PII:**

Application read and process PII across the workflows. Application has the ability to import DICOM data containing PII. During the further workflow application have ability to update and include PII data in planning summary document. Application does not update the source DICOM data. As a part of safety measures application shows PII on each workflow step. Application also maintains the previous case lists on local drive. This case list file is encrypted and stored on windows user directory.

**Access control measure:**

PII data is stored in windows user directory and is not accessible to other users.

**Data Security measures:**

Files stored on the local drive containing PII is encrypted with 256-bit AES (Advanced Encryption Standard). Only authorized users having Thor Application can decrypt the files. Other users can use their key to decrypt files.

Audit logs containing the PII are encrypted. Decryption of the audit log is handled by Stryker on request from authorities.

**Data Anonymization measures:**

Application have ability to anonymize the PII shown on the application GUI on demand.

**Management of PHI:**

Application have ability to read, process and update the PHI. However, the application does not update the source DICOM data. PHI is stored in MITK files and planning summary files.

**Access control measure:**

PHI data is stored in windows user directory and is not accessible to other users.

* The display of PII (e.g., video display, etc.)

Application displays PII information on workflow steps as a part of safety measures. Application have ability to anonymize the PII data on display.

* Generation of hardcopy reports or images containing PII

Application includes the PII data in planning summary document which can be printed or transmitted.

# AUTOMATIC LOGOFF

Kneebalancer application does not have an ability to lock the device after being idle for certain time period. MPS users are advised to configure iOS device to automatically lock the screen after a reasonable period of time as per Stryker IT policies.

# AUDIT CONTROLS

The Kneebalancer application have ability to capture and store events such as application’s crash logs, case data logs, device logs. These logs are stored on the device in the application’s sandbox directories. These logs are accessible to Kneebalancer application only.

The audit logs do not contain any sensitive information or PII or PHI. MPS users are not required to take any special measures to protect these logs. The audit logs are uploaded along with case data and stored in Stryker’s cloud with the security and encryption as provided by the Microsoft Azure. These logs are removed from the device within period of 30 days if not uploaded on the Stryker’s cloud. The logs are deleted from the device once they are uploaded to the Stryker’s cloud.

# AUTHORIZATION

Kneebalancer application can be installed via authorized entity of Stryker only. The application can be installed from the Stryker’s app store on the Stryker devices only. Stryker admin must give permissions for the MPS user to install the Kneebalancer application through Stryker app store. After installation, the Kneebalancer application is enabled for single user that is the MPS user of the device. Hence, no authorization is required to access the application. Case data created by the single MPS user is uploaded on Stryker’s cloud using the MPS user’s Stryker credentials.

As the Kneebalancer application is enabled for the authorized (MPS) user. Hence, there is no requirement of role-based access control within the application.

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

# CYBER SECURITY PRODUCT UPGRADES

***Existing Security Features:***The Kneebalancer application does not have any updates installation policy implemented. Hence, the MPS users will not get any notification of online updates. If Stryker identifies any potential vulnerabilities which require an update of the application, new version of the Kneebalancer application will be released and MPS users will be informed about the action to be taken at their end.

***Recommendation for MPS users:*** Any information regarding cyber security product upgrades can be requested from Stryker.

# HEALTH DATA DE-IDENTIFICATION

Kneebalancer does not collect/store/process any health data. Hence, option for the health data de-identification is not required.MPS user MPS user

# DATA BACKUP AND DISASTER RECOVERY

The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. The case data gets uploaded on the Stryker’s cloud. The Kneebalancer application does not contain any online or offline mode of data on device or its recovery.

# EMERGENCY ACCESS

Kneebalancer application doesn’t contain the patient personal details. Hence no option for the device user (MPS) to access personally identifiable information in case of a medical emergency that requires immediate access to stored personally identifiable information.

# HEALTH DATA INTEGRITY AND AUTHENTICITY

Kneebalancer application do not store any kind of health data on the device. Hence, health data integrity and authenticity is not applicable in case of Kneebalancer application.~~MPS user~~

# MALWARE DETECTION/PROTECTION

***Existing Security Features:***By default, the standalone Kneebalancer application does not have any malware detection features and it is the responsibility of Stryker, as the device is owned by the Stryker. To protect against the malwares below points are recommended:

***Recommendation for MPS users:***

* Keep your iOS device and installed application updated.
* Use strong password/pin code to unlock the device.
* Do not click on any URLs or download anything from the internet or received via airdrop.
* Limit your file-sharing over internet or locally via airdrop.
* Be careful about opening email attachments or images. Configure the mail server to restrict auto download or auto rendering of images received in emails outside organization.

# NODE AUTHENTICATION

Node authentication is required when communication happens between multiple devices within the environment. The Kneebalancer application does not require to communicate with multiple devices. Hence, node authentication is not required in the Kneebalancer application.

# CONNECTIVITY CAPABILITIES

The Kneebalancer application has the ability to connect to the network for uploading case data.

# Communication Provisions

The Kneebalancer application has ability to connect to network via wireless connectivity feature. The connection is made in order to communicate with Stryker’s cloud to store case data, audit/debug logs on the Stryker’s cloud. The Kneebalancer application has ability to make API calls back and forth to transfer the data mentioned above. These API calls are used to upload case data to the Stryker’s cloud. The data is transmitted and stored on Stryker’s cloud with the security and encryption as provided by the cloud service provider.

# PERSON AUTHENTICATION

Only the Stryker's iOS devices can be used to install the Kneebalancer application via Stryker’s app store. Moreover, Stryker admin must give permissions for the MPS user to install the Kneebalancer application through Stryker app store.

During the case data upload to Stryker’s cloud, Kneebalancer application has the ability to authenticate the MPS user. This authentication is done via Stryker’s credentials of the MPS user.

# PHYSICAL LOCKS

Physical locks are not required for this product.

# ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE

The Kneebalancer application uses the iOS platform which publishes the apps with greater security from the manufacturer using provisioning files and certificates.

**Recommendation for MPS user:** Any information regarding Roadmap for Third Party Components in Device Life Cycle can be requested from Stryker.

# SOFTWARE BILL OF MATERIALS

It is addressed in the Software Architecture Document (SAD).

# SYSTEM AND APPLICATION HARDENING

Stryker had performed the application security testing and security code review of Kneebalancer application. Kneebalancer application is hardened by eliminating any vulnerability or flaw, which can lead to security issue. Kneebalancer application runs on a Stryker provided mobile device, hence Stryker policies are applicable and hardened as per procedures.

# HEALTH DATA STORAGE CONFIDENTIALITY

The Kneebalancer application does not collect/store/process any health data. Hence, health data storage confidentiality is not considered in the Kneebalancer application.

# TRANSMISSION CONFIDENTIALITY

Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Kneebalancer application transmits the data over the network via pre-identified end point (Stryker’s cloud) configured API calls. These API calls are transmitted over secure channel. The data transmission happens over the network and the encryption for the data is provided by Stryker’s cloud.

# TRANSMISSION INTEGRITY

The Kneebalancer application uploads case data to the Stryker’s cloud after the authentication through a secure HTTPS network.

# REMOTE SERVICE

Kneebalancer application does not require remote service for any functionality or for the application itself.

# SECURITY PROGRAM INTEGRATION

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

# Vulnerability Management

When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability’s exploitability and impact is conducted. Based upon this assessment Stryker determines if further actions are required like providing security updates and/or providing communication to the MPS users in a timely manner. Vulnerability information may also be requested from Stryker at any time.

# Incident Response

***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 on the assessment report, Stryker determines if further actions similar to providing security updates and/or providing information to the MPS users 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 (device/tablet) 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 MPS user:**

* MPS user is recommended to be up to date with the software being used and latest Stryker provided hardware (device/tablet).

**Training and Awareness:**

* MPS users utilizing the devices should be provided with proper training including their functionality.

***Recommendation for*** ***MPS user:*** MPS users 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 Technical Team.

# Security Testing

The product is installed on an iOS operating system, and Stryker has evaluated that standard security testing methodologies commonly employed for the Operating System type are appropriate. No special procedures for security testing are required beyond those typically applied to the Operating System.

# Scanning

The Kneebalancer application requires the proper authentication to communicate over the internet for the data transfer. Also, Stryker has already done extensive security testing of the Kneebalancer application at the time of release. However, beyond this security measures in place it is advised for the MPS users to take a step ahead and follow some of the below guidelines to ensure better security postures:

* Do not connect to any public or open wireless network. Only connect the device to trusted wireless network. Also, do not connect to any wireless network which has enabled old or outdated protocols such as WEP2.
* Do not connect to any insecure wireless interfaces such as Bluetooth, NFC etc.
* Do not install any application from place other than Stryker’s Appstore. Also, do not install unnecessary applications in the device.

# Risk Management

As a part of Risk management, Risk assessment is conducted within the organization (Stryker) to identify the gaps and planned improvements incorporated.

# Training and Awareness

Stryker has evaluated the security training requirements for this product and determined that standard MPS user security and awareness training commonly provided to MPS users of general-purpose business environments is sufficient for standard MPS users. This general security awareness may include the below points:

* Do not connect to any public or open wireless network. Only join a reliable wireless network with the device. Additionally, avoid using any wireless networks that have WEP2 enabled if possible.
* Along with wireless network interfaces, do not connect and communicate with other insecure or public wireless interfaces such as Bluetooth, NFC, airdrop communication
* Use strong pin or passcode to unlock the device. This reduces the risk of unattended device access.
* While device is connected to the internet, do not click on any unknown link’s, or do not download any files that may be a potential security threat to the system as well as to the application.
* Do not connect any external drive such as USB drive via OTG cable or plug to the device. Do not connect the charging interface to insecure connection port.

# SECURE DECOMMISSIONING

For secure decommissioning of Kneebalancer refer to User Manual.

In case of any further information required, please reach out to Stryker Customer Care for secured decommissioning of Stryker owned Kneebalancer components such as (iOS device, tablet).

# Appendix

# List of 3rd party components:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | Manufacturer | Version | Release Date | License Type | Maintenance procedure |
| MITK | MITK | 2018.04.02 | 13/03/2019 | BSD | Dynamically linked, Embedded in product |
| Qt | Qt | 5.11 | 22/05/2018 | Qt Commercial License, GPL 2.0, 3.0, LGPL 3.0 | Dynamically linked, Embedded in product |
| VTK | VTK.org | 8.1 | 22/12/2017 | BSD | Dynamically linked, Embedded in product |
| ITK | ITK community | 4.13.1 | 13/08/2018 | Apache 2.0 license | Dynamically linked, Embedded in product |
| CTK | Commontk.org | 0.1.0 |  | Apache 2.0 license | Dynamically linked, Embedded in product |
| Log4cpp | Lifeline Networks bv | 1.1.1 | 26/11/2013 | GNU Lesser General Public License. | Dynamically linked, Embedded in product |
| boost | boost | 1.69.0 | 12/12/2018 | Boost software license | Dynamically linked, Embedded in product |
| tiff | Adobe | 4.0.7 |  |  | Dynamically linked, Embedded in product |
| teem |  | 1.11.0.5 |  | GNU Lesser General Public License. | Dynamically linked, Embedded in product |
| minizip | zlib | 1.1 |  | zlib license | Dynamically linked, Embedded in product |
| cppunit |  | 1.14.1 |  | GNU Lesser General Public License. | Dynamically linked, Embedded in product |
| tinyxml2 | zlib | 4.0.1 |  | zlib license | Dynamically linked, Embedded in product |
| opencv | Opencv.org | 4.1.0 | 8/04/2019 | open-source Apache 2 License | Dynamically linked, Embedded in product |
| DCMTK | Dcmtk.org | 3.6.4 | 30/11/2018 | BSD | Dynamically linked, Embedded in product |
| OpennGL | The Khronos Group |  |  | BSD | Dynamically linked, Embedded in product |