Document Approval:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Issued by:  Quality |  | Sreejith Viswam |  |  |  |  |  |
|  | Name printed |  | Signature |  | Date |  |
| Revision No.: |  | | | | | | |
| Approved by  PL: |  | Diksha Babhoota |  |  |  |  |  |
|  | Name printed |  | Signature |  | Date |  |
| Approved by  TEST: |  | Imon Dey |  |  |  |  |  |
|  | Name printed |  | Signature |  | Date |  |
| Approved by  QA: |  | Sreejith Viswam |  |  |  |  |  |
|  | Name printed |  | Signature |  | Date |  |
| Approved by  Development: |  | Sridhar Manickavel |  |  |  |  |  |
|  | Name printed |  | Signature |  | Date |  |

# Document Revision History:

|  |  |  |  |
| --- | --- | --- | --- |
| Revision  Level | Revision Date | Reason for change | Author |
| 00 | 11 Sept 2022 | Initial Release | Sreejith Viswam |
| 01 |  |  |  |

**Kneebalancer**

**Security Operations Manual**

This document was prepared by Knee Balancer development team of Stryker’s Global Technology Center Private Limited, India. See section 3.1 below for contact information.

**Table of Contents**

[1. PURPOSE 5](#_Toc114668709)

[2. DEFINITIONS 5](#_Toc114668710)

[3. PRODUCT DESCRIPTION 7](#_Toc114668711)

[3.1 Product and Manufacturer Identification 7](#_Toc114668712)

[3.2 Product Intended Use 7](#_Toc114668713)

[3.3 Related Manufacturer Programs 7](#_Toc114668714)

[3.4 System Characterization and System Assets 8](#_Toc114668715)

[3.5 System Security Context and Intended Environment 8](#_Toc114668716)

[3.6 Network, Data Flow Diagram 9](#_Toc114668717)

[4. MANAGEMENT OF PII and PHI 9](#_Toc114668718)

[5. AUTOMATIC LOGOFF 10](#_Toc114668719)

[6. AUDIT CONTROLS 10](#_Toc114668720)

[7. AUTHORIZATION 10](#_Toc114668721)

[8. CYBER SECURITY PRODUCT UPGRADES 10](#_Toc114668722)

[9. HEALTH DATA DE-IDENTIFICATION 10](#_Toc114668723)

[10. DATA BACKUP AND DISASTER RECOVERY 11](#_Toc114668724)

[11. EMERGENCY ACCESS 11](#_Toc114668725)

[12. HEALTH DATA INTEGRITY AND AUTHENTICITY 11](#_Toc114668726)

[13. MALWARE DETECTION/PROTECTION 11](#_Toc114668727)

[14. NODE AUTHENTICATION 11](#_Toc114668728)

[15. CONNECTIVITY CAPABILITIES 11](#_Toc114668729)

[15.1 Communication Provisions 11](#_Toc114668730)

[16. PERSON AUTHENTICATION 12](#_Toc114668731)

[17. PHYSICAL LOCKS 12](#_Toc114668732)

[18. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE 12](#_Toc114668733)

[19. SOFTWARE BILL OF MATERIALS 12](#_Toc114668734)

[20. SYSTEM AND APPLICATION HARDENING 12](#_Toc114668735)

[21. HEALTH DATA STORAGE CONFIDENTIALITY 12](#_Toc114668736)

[22. TRANSMISSION CONFIDENTIALITY 13](#_Toc114668737)

[23. TRANSMISSION INTEGRITY 13](#_Toc114668738)

[24. REMOTE SERVICE 13](#_Toc114668739)

[25. SECURITY PROGRAM INTEGRATION 13](#_Toc114668740)

[25.1 Vulnerability Management 13](#_Toc114668741)

[25.2 Incident Response 13](#_Toc114668742)

[25.3 Security Testing 13](#_Toc114668743)

[25.4 Scanning 14](#_Toc114668744)

[25.5 Risk Management 14](#_Toc114668745)

[25.6 Training and Awareness 14](#_Toc114668746)

[26. SECURE DECOMMISSIONING 14](#_Toc114668747)

# PURPOSE

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

This manual 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 also the completed case data details to the Azure blob storage with the user consent and the internet availability.

**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.

**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 Kneebalancer application on behalf of surgeon. Creates initial planning and inputs the planning values to Kneebalancer application to generate gap solution is performed by MPS user. Based on the discussion with surgeon, MPS user updates the values in the Mako system.

**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 a software not developed by Stryker, and for which Stryker otherwise does not have complete ownership.

**User**: Refer-MPS user.

**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 potential 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 Kneebalancer 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. MPS user creates initial planning and inputs the planning values to Kneebalancer 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 also the completed case data details to the Azure blob storage with the user consent and the internet availability.

# System Security Context and Intended Environment

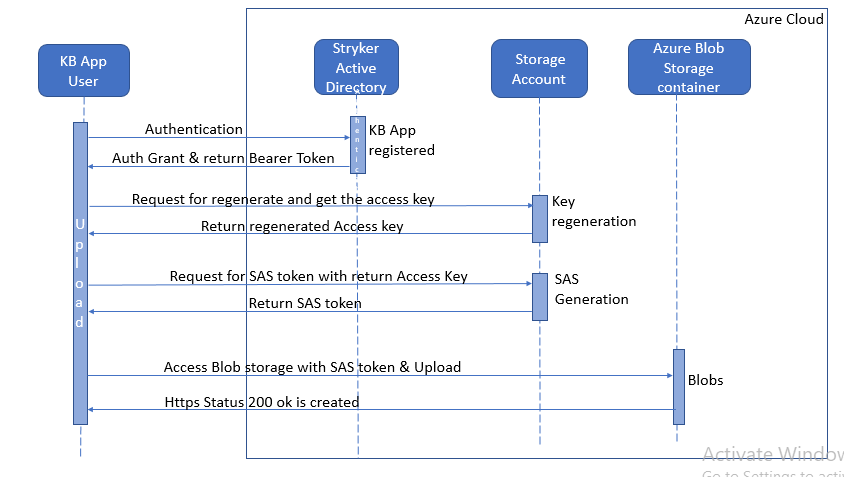


There is no requirement for the Kneebalancer application to work in an environment or function other than iOS operating system. Hence, the application is designed to work completely within iOS device boundary. However, Stryker recommends the MPS user to follow some of the best security standards in order 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 is required for MPS user.

# 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 Information 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, and device logs. These logs are stored in the secured location and are accessible to the Kneebalancer application.

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 after uploading 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 store on the Stryker devices only. Stryker admin must give permissions for the MPS user to install the Kneebalancer application through Stryker store. After installation, the Kneebalancer application is enabled for single user i.e., 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 requires 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 Kneebalancer application does not contain any online or offline mode of data on device or its recovery. The case data gets uploaded on the Stryker’s cloud.

# EMERGENCY ACCESS

Kneebalancer application doesn’t contain any patient’s 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 doesn’t have any malware detection features and it is the responsibility of Stryker, as the device is owned by the Stryker. To protect against the malware below points are recommended:

***Recommendation for MPS users:***

* Keep your iOS device and installed application updated.
* Use strong password/pin code to lock/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 from unknown persons/external sources.

# 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 store. Moreover, Stryker admin must give permissions for the MPS user to install the Kneebalancer application through Stryker 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

**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 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 doesn’t get considered/applies for Kneebalancer application.

# TRANSMISSION CONFIDENTIALITY

Kneebalancer application transmits the data over the internet 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 doesn’t require remote service for any functionality or for the application itself.

# SECURITY PROGRAM INTEGRATION

This section provides configuration guidelines for the MPS users to enable/achieve compliance during the product/application integration.

# Vulnerability Management

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.

# Incident Response

* ***Recommendation for*** ***MPS user:*** MPS users is recommended to be up to date with the software being used and latest Stryker provided hardware device. 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, please reach out to 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

Scanning is not required for this product.

# 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

On needed basis, if required Stryker can provide the training for the MPS user. However, this manual can be referred for security awareness with Kneebalancer application.

* Try to avoid installing applications other than the legitimate Stryker store.
* MPS user should abide to Stryker security policies and follow procedures such as use strong pin or passcode to lock/unlock the MPS user device.
* While device is connected to the internet, do not click on any unknown link, or do not download any files that may be a potential security threat to the device as well as to the application.

# 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 (device).