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 |  |  |  |

**Knee Balancer**

**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 6](#_Toc113813055)

[2. DEFINITIONS 6](#_Toc113813056)

[3. PRODUCT DESCRIPTION 9](#_Toc113813057)

[3.1 Device and Manufacturer Identification 9](#_Toc113813058)

[3.2 Device Intended Use 9](#_Toc113813059)

[3.3 Vulnerability Intake and Monitoring 9](#_Toc113813060)

[3.4 System Characterization and System Assets 9](#_Toc113813061)

[3.5 System Security Context and Intended Environment 10](#_Toc113813062)

[3.6 Network, Data Flow Diagram 11](#_Toc113813063)

[3.7 Setup of SaMD 11](#_Toc113813064)

[4. MANAGEMENT OF PII and PHI 12](#_Toc113813065)

[4.1 Authority to Collect PHI 12](#_Toc113813066)

[4.2 Purpose Specification for PHI Use 12](#_Toc113813067)

[4.3 PHI Data Quality and Integrity 12](#_Toc113813068)

[4.4 PHI Data Deletion and Minimization 12](#_Toc113813069)

[4.5 Legal Roles and Related Requirements for Privacy 12](#_Toc113813070)

[4.6 Handling of Patient Requests for their PHI Access 12](#_Toc113813071)

[4.7 Storage and Removal of PII 12](#_Toc113813072)

[4.8 Transmitting, Importing/Exporting of PII 12](#_Toc113813073)

[5. AUTOMATIC LOGOFF 12](#_Toc113813074)

[6. AUDIT CONTROLS 13](#_Toc113813075)

[6.1 Device-Specific Audit Log Configuration 13](#_Toc113813076)

[6.2 Events and Attributes Recorded 13](#_Toc113813077)

[6.3 Audit Log Protection 13](#_Toc113813078)

[6.4 Log Export, Use, and Notification 14](#_Toc113813079)

[7. AUTHORIZATION 14](#_Toc113813080)

[7.1 Access Prevention 14](#_Toc113813081)

[7.2 Privilege and Access 15](#_Toc113813082)

[7.3 System Use Notification 16](#_Toc113813083)

[8. CYBER SECURITY PRODUCT UPGRADES 16](#_Toc113813084)

[8.1 Secure Servicing and Security Upgrades Overview 16](#_Toc113813085)

[8.2 General Parameters for Updates 16](#_Toc113813086)

[8.3 Operating System Updates 17](#_Toc113813087)

[8.4 Driver, Firmware Updates 17](#_Toc113813088)

[8.5 Anti-Malware Software Updates 17](#_Toc113813089)

[8.6 COTS (non-OS) Updates 18](#_Toc113813090)

[8.7 Other Software Component Updates 18](#_Toc113813091)

[9. HEALTH DATA DE-IDENTIFICATION 18](#_Toc113813092)

[10. DATA BACKUP AND DISASTER RECOVERY 18](#_Toc113813093)

[11. EMERGENCY ACCESS 18](#_Toc113813094)

[12. HEALTH DATA INTEGRITY AND AUTHENTICITY 18](#_Toc113813095)

[13. MALWARE DETECTION/PROTECTION 19](#_Toc113813096)

[13.1 Support of Anti-Malware 19](#_Toc113813097)

[14. NODE AUTHENTICATION 19](#_Toc113813098)

[15. CONNECTIVITY CAPABILITIES 19](#_Toc113813099)

[15.1 Hardware Connectivity Capabilities 20](#_Toc113813100)

[15.2 Communication Provisions 20](#_Toc113813101)

[16. PERSON AUTHENTICATION 20](#_Toc113813102)

[16.1 Password/ID Assignments 20](#_Toc113813103)

[16.2 User Account Management 21](#_Toc113813104)

[17. PHYSICAL LOCKS 21](#_Toc113813105)

[18. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE 21](#_Toc113813106)

[19. SOFTWARE BILL OF MATERIALS 21](#_Toc113813107)

[19.1 SBoM Structure and Updates 21](#_Toc113813108)

[20. SYSTEM AND APPLICATION HARDENING 21](#_Toc113813109)

[21. HEALTH DATA STORAGE CONFIDENTIALITY 22](#_Toc113813110)

[22. TRANSMISSION CONFIDENTIALITY 23](#_Toc113813111)

[23. TRANSMISSION INTEGRITY 24](#_Toc113813112)

[24. REMOTE SERVICE 24](#_Toc113813113)

[25. SECURITY PROGRAM INTEGRATION 24](#_Toc113813114)

[25.1 Vulnerability Management 24](#_Toc113813115)

[25.2 Incident Response 24](#_Toc113813116)

[25.3 Security Testing 26](#_Toc113813117)

[25.4 Scanning 26](#_Toc113813118)

[25.5 Risk Management 26](#_Toc113813119)

[25.6 Training and Awareness 26](#_Toc113813120)

[26. SECURE DECOMMISSIONING 27](#_Toc113813121)

[27. Appendix 28](#_Toc113813122)

[27.1 List of 3rd party components: 28](#_Toc113813123)

# PURPOSE

This Security Operations Manual (SOM) provides information that Stryker’s customers need to integrate a specific Stryker device or health IT solution into a customer’s IT network environment. It also supports a customer’s ability to perform risk management, to identify configurable security controls, and to better protect their systems and devices.

# DEFINITIONS

**AAMI – Association for the Advancement of Medical Instrumentation**: An organization for advancing the development, and safe and effective use of medical technology. AAMI publishes standards and technical reports related to various aspects of medical device development and use (e.g., AAMI TIR57). See www.aami.org.

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

**COTS – Commercial off-the-shelf**: Software (or any other item) that is sold as a packaged solution which is then adapted to satisfy the needs of the organization purchasing the COTS. Some medical devices utilize COTS software in addition to or instead of software developed by the manufacturer. See third-party software.

**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.

**FDA – U.S. Food and Drug Administration:** A federal agency of the United States’ Department of Health and Human Services. See www.fda.gov.

**MPS User- Mako Product Specialist User:** MPS is the user of the Knee Balancer application who inputs the planning parameters from MAKO planning laptop/MAKO robotic system and gaps/laxity values which are available from ligament assessment. These parameters are input to Knee Balancer application in order to generate gap solution. Based on the discussion with surgeon, MPS user updates the solution in the Mako system.

**IEC – International Electrotechnical Commission**: A global organization whose work underpins quality infrastructure and international trade in electronic goods. IEC publishes thousands of international standards, including documents related to medical device software (e.g., IEC 62304). See www.iec.ch.

**ISAO – Information Sharing and Analysis Organization:** An ISAO is any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability (source: from NIST SP 800-150).

**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. See https://ec.europa.eu/health/md\_sector/overview

**Medical Device:** See the following sources if a precise definition is required: FDA, MDR (EU) 2017/745, ISO 14971:2007.

**NIST - National Institute of Standards and Technology**: A physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. NIST has published comprehensive standards for the selection, implementation, and risk management of security and privacy controls (e.g., NIST SP 800-53). See www.nist.gov.

**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).

**OSS – Open-Source Software**: Third party software licensed under an OSS license, in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose as long as the license terms are adhered to.

**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 (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:** See Device.

**SaMD - Software as a Medical Device**: Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (source: from International Medical Device Regulators Forum).

**SBoM – Software Bill of Materials**: For a specific device, a listing of all software components that are incorporated into the final product. The SBOM may be used to assist with operational security planning by the MPS.

**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.

**SOUP**: Software of Unknown Provenances

# PRODUCT DESCRIPTION

|  |  |
| --- | --- |
| **Manufacturer Name** |  |
| **Stryker Division** | Stryker Global Technology Center Private Limited |
| **Address** | Vatika Business Park, 10th Floor, Block 2, Sector 49, Sohna Road, Gurgaon, 122002, Haryana, India |
| **Device Description** | Knee balancer application |
| **Device Model, Version** | Refer to Software “About” section in the application |
| **Manufacturer Contact Information** | Stryker Global Technology Center Private Limited |

# Device and Manufacturer Identification

# Device Intended Use

The Knee Balancer application is intended as a clinical decision support system that provides planning assistance for Total Knee Arthroplasty (TKA) procedures.

The system is indicated for conditions of the knee joint in which the use of robotics may be appropriate.

The system supports the following surgical knee procedures:

- Total Knee Arthroplasty (TKA)

# 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 customer in a timely manner. Vulnerability information may also be requested from Stryker at any time.

Stryker participates in the **MedTech Information Sharing and Analysis Organization** (ISAO), a part of **AdvaMed** (Advanced Medical Technology Association).

Any potential security vulnerabilities due to Knee balancer application which users become aware of shall be initiated as a complaint and the same will be handled through the post market complaints management process to do the assessment and required actions including any updates needed for the User devices.

# System Characterization and System Assets

The Knee Balancer application is intended as a clinical decision support system that provides planning assistance for Total Knee Arthroplasty (TKA) procedures. The application do not store any PII and PHI information. On completion of case, related data and logs are uploaded to Stryker cloud. The data stored in cloud do not contain any PHI/PII and can only be used for post market complaint assessments on if the application output is accurate for the inputs provided for a specific MPS user who used the application for a case. The inputs and output stored do not include PII/PHI information.

# System Security Context and Intended Environment



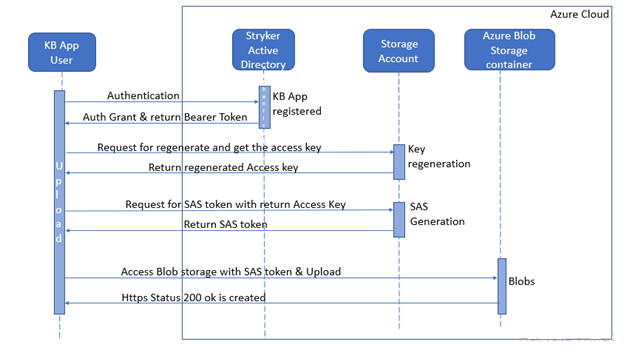
While there is no specific requirement for Knee balancer application to be fully functional other than a usual iOS environment, however Stryker recommends the user to follow some of the best security standards in order to run the application in a safe and secure environment as follows:

However, Stryker recommends the MPS user to follow some of the best security standards as mentioned below in order to run the application in a safe and secure environment -

* MPS shall abide by the Stryker IT policies on usage.
* MPS user login credentials should be secured and follow Stryker policies while creating passwords for device.
* 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 Knee Balancer application to prevent danger of using vulnerable software/OS.
* MPS shall never leave the device unattended in unlocked state.

# Network, Data Flow Diagram

High level data flow diagram.



# Setup of SaMD

Knee Balancer application is only installed on a Stryker Managed Mako Product Specialist IPhone / IPad which utilizes iOS as operating system. The application is installed from Stryker App Store based on authorization of the specific users for installation. Other unauthorized users will not be able to see Knee Balancer Application for download in the Stryker App Store.While there is no specific requirement for Knee balancer application to be fully functional other than a usual iOS environment, however Stryker recommends the user to follow some While there is no specific requirement for Knee balancer application to be fully functional other than a usual iOS environment, however Stryker recommends the user to follow some

# MANAGEMENT OF PII and PHI

Knee Balancer application does not collect or ask user for any PII or PHI. Thus, no PII or PHI is created or stored in the device. This section is not applicable.

**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

Application do not lock the device after being idle for certain time period. Customers are advised to configure iOS device to automatically lock the screen after a reasonable period of time to prevent misuse.

# AUDIT CONTROLS

The Knee Balancer application have ability to capture and store important event and actions as part of audit logs. These logs are stored on the device and are accessible to Knee Balancer application. Any other application installed on same device or user of the device cannot access or does not have control over these logs. Audit logs are an important part of any secure system, and they need to be carefully designed in order to give a faithful representation of past system activity.

The audit logs do not contain any sensitive information or PII or PHI. Users are not required to take any special measures to protect these logs but are not restricted from doing the same. The audit logs are uploaded along with case data (no PII or PHI is included) and stored in Azure cloud with the security and encryption as provided by the Azure cloud. These logs are removed from the device after uploading to the storage server of Stryker.

# Device-Specific Audit Log Configuration

The application captures the audit logs and stores in the specific secure location on the device. Audit logs are not configurable by user. No PII is logged in these audit logs.

# Events and Attributes Recorded

Application captures the errors and exceptions in JSON format. These logs only contain errors and exception occurred in device and the Knee Balancer application. Logs are pushed to cloud whenever the device comes online and if there is past case data waiting for upload. As soon as user provides his credentials and if past case data is available, all the logs are pushed to cloud. Any sort of user information is not logged in these events and attributes being recorded in these logs. Log details will be stored with combination of error details, crashing details, exception details, and event logs. The events and attributes recorded in these log files are as below:

* Application/Device errors
* Application/ Device exceptions
* Case data logs
* Event logs (Tracking)

# Audit Log Protection

The audit logs are captured and stored in the specific location in the device and are accessible to the application only. The user of device or any other app installed on the same device do not have any control over these logs. These logs are not protected by any protection mechanism as they are stored in secure mechanism at first place. Moreover, these logs do not contain any sensitive or PII/PHI data.

These logs get uploaded on the Stryker’s storage server along with the case data. Once they are uploaded on the storage server, they are removed from the local memory of the device. The logs also contain debug errors and reports of the device and the application which also gets removed once uploaded on the Stryker’s server. The audit logs are transmitted and stored in Azure cloud with the security and encryption as provided by the Azure cloud. The application prevent the users to use the same unless these logs are uploaded on storage server of Stryker within 30 days.

# Log Export, Use, and Notification

Knee Balancer application does not have any built-in feature to store backup of logs (like in case of data deletion). It is also not possible to export these logs using any wireless or physical media as these logs are only accessible to Knee Balancer application only.

The logs contain specific actions of the application, crash reports, debug reports and errors, application’s behavioral reports which are stored on the local storage on the device in specific location assigned to Knee Balancer application only. These logs are isolated from users of device and any other app on same device and are limited to Knee Balancer application only.

# AUTHORIZATION

Knee Balancer application can be installed via authorized entity of Stryker. Once installed, application does not enforce any authorization mechanism to access the application. The application is installed on Stryker’s authorized devices via Stryker’s app store only and Stryker admin must approve the installation of the Knee Balancer application on Stryker’s device. A single user can log in via *Microsoft Authentication Library (MSAL)* mechanism on the device to upload case data to the Stryker’s storage servers.

Authorization in system security is the process of giving the user permission to access a specific resource or function. In secure environments, authorization must always follow authentication. In order to upload the case data on the server, the user is required to login into the application via Single sign on authentication mechanism with their own account.

# Access Prevention

This section is not applicable as a single user can be logged in into the application via single sign on authentication mechanism to use features of the application such as case data upload.

However, taking steps to prevent unauthorized access to the device and its software components is important for a wide number of reasons, including preventing unauthorized malicious actors from installing spyware, malware and deleting your important files, or further creating viruses. By making changes to your iOS devices to prevent unauthorized access, you are also protecting your personal privacy. Here are some steps to take to properly secure your iOS device and prevent others from accessing or modifying your application data:

* Set password/pin protection for unlocking the device: The iOS device must be protected with password, pin, or any other kind of authentication to prevent unauthorized parties from unlocking the device.
* Strong password/pin protection for device: The implemented authentication mechanism such as password, pin etc. must be set in such way that it must not be easy to guess.
* Install any applications from Appstore of Apple and Stryker devices only. This will ensure installation of un-tampered applications. Additionally, install only required applications in your iOS device. This will also prevent any malicious or spyware application installation which are usually bundled or hidden in the normal applications.
* Restrict the access to your iOS device to other peoples. This can help the installed application to be accessed only by an authorized individual.
* Keep your Apple ID secure. Your iCloud data and account details for services like the App Store and Apple Music are accessible through your Apple ID. Keep your Apple ID secure on iPhone to prevent any unauthorized access to data on iCloud and access to some of the features of device such as location information, notifications, personal information etc.
* Do not connect to any unknown wireless network to use the internet services.
* Do not connect to any untrusted Bluetooth devices. Further keep Bluetooth option disabled if not being utilized.

# Privilege and Access

Privilege, in the context of security, is the concept of only allowing users to do certain things. For example, an ordinary user is typically prevented from changing operating system files, while a system administrator is typically permitted to do so. As the Knee Balancer application do not have multiple access roles, this section is not applicable.*, I If the device is integrated with enterprise or upstream identity and access management capability, describe that here.*

# System Use Notification

This section is not applicable

*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 Knee Balancer application will be updated in Stryker Appstore with a next version if Stryker identifies any potential vulnerabilities which require an update. The users will have an updated version available for installation and ensure to update the application whenever a new version is available.

***Recommendation for customer (MPS):*** Any information regarding cyber security product upgrades can be requested from Stryker if the users come to know about any possible cyber security risks.

# Secure Servicing and Security Upgrades Overview

The application update is possible only at the next release of the application which depends on major/minor changes such as features, security fixes, etc. The users are recommended to upgrade to the latest version whenever an update is available for Knee Balancer application in the Stryker AppStore. However, it is recommended for the users to apply their operating system patches and their third-party components (if any) to maintain the system security.

Apple usually release security updates for iOS as soon as issues are patched. These updates address various bugs and vulnerabilities which are being exploited in the wild. Security updates are just patches which comes with feature enhancements, performance improvement, bug fixes, etc. General bug fix update is usually between 6 months and the major update in iOS generally pushed every 1-1.5 years.

On patching these security updates, your device will become more secure with enhanced protection as well as performance.

# General Parameters for Updates

Note: This section is Not Applicable

# Operating System Updates

Outdated operating system is the weakest links. It is recommended for the users to keep your Apple iOS updated to ensure the device running smoothly and securely. When you update, you’ll get the latest fixes and security improvements, helping your device run efficiently and stay protected. Important and high-priority updates are critical to the security and reliability of your iOS device. Updates offer the latest protection against malicious online activities. Not keeping your operating system up to date can result in serious issue, affecting both your device and your own personal security. These include:

* Vulnerable OS components due to missing patches.
* Crashing, lagging, basically poor performance.
* Various viruses, spyware, malicious threat actors and other malwares
* Various cybercrime attacks
* Incompatibility for certain security features which are available in antivirus apps but unable to implement due to old and incompatible OS version.

# Driver, Firmware Updates

Note: This section is Not Applicable

# Anti-Malware Software Updates

Knee Balancer application does not contains any malware protection embedded. Thus, users are expected to take care of the installations and configuration of anti-malware software themselves. An anti-malware is a software/application that protects the device from various malware such as adware, worms, crypto mining malware, spyware, etc. Anti-malware application scans the device and OS components for all types of malicious software applications, outdated software, among all of the installed applications or hidden inside any application which manage to reach to the device.

The software updates of anti-malware comprise of latest files needed to combat the latest threats and safeguard your device. Hence, it is really important to update these applications as soon as updates are available for them. If these applications are not updated for long time, it is like not having them on the device.

As the database of anti-malware application is regularly gets updated with signatures and information of latest threats, malware, spywares etc. Thus, updating these applications also helps you to detect any recent malware installed into your iOS device. As iOS itself offers lots of security features to battle against those malwares however, it is highly recommended to purchase and use any good anti-malware application to avoid any slip of malware due to misconfiguration of security feature offered in iOS.

# COTS (non-OS) Updates

Note: This section is Not Applicable

# Other Software Component Updates

Note: This section is Not Applicable

# HEALTH DATA DE-IDENTIFICATION

Knee Balancer application does not collect or store any sensitive information or PII or health data of the user. Thus, this section is not applicable.

# DATA BACKUP AND DISASTER RECOVERY

The application does not contain any online or offline mode of data on device or its recovery. The purpose of the backup is to create a copy of data that can be recovered in the event of any complaints for the investigation purpose. The case data gets uploaded on the azure storage server of Stryker once, user is logged-into the application.

# EMERGENCY ACCESS

Note: This section is Not Applicable

# HEALTH DATA INTEGRITY AND AUTHENTICITY

The application does not store any sensitive information on the iOS device or on the Stryker’s server. Thus, this section is not applicable.

# MALWARE DETECTION/PROTECTION

By default, the standalone Knee Balancer application does not have any malware detection features and requires the user to have some malware detection in place in their iOS device. Due to the ubiquity of malware, malware detection is essential since it serves as an iOS device’s early warning system for malware and cyberattacks. It stops hackers from remotely accessing the device and guards against data breaches. To do this, an iOS device and its files must be scanned for malware. To protect against the malwares below points are recommended:

* Keep your iOS device and installed application updated. Auto update feature must be enabled in Appstore and in device’s settings
* 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
* Install a good malware detection and mitigation application on the device
* 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.
* Always download applications from Apple’s Appstore. Moreover, install only required application on the device.
* Do not provide any unnecessary permissions (to access system component, data) to any other installed application.

# Support of Anti-Malware

The application does not contain any anti-malware functionality within itself. Also, it does not restrict users to install any types of anti-malware programs supported by their operating system. Hence, users are best recommended to install some of the popular anti-malware programs on their own.

# NODE AUTHENTICATION

As application do not have any ability to communicate between multiple devices, this section is not applicable.

# CONNECTIVITY CAPABILITIES

All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.

# Hardware Connectivity Capabilities

The application does not require to be connected to any physical media in order to operate and does not apply any restrictions in place for the same. Users are advised to connect to secure wireless connections only if accessing the internet through wireless network.

# Communication Provisions

The application only requires internet connection to communicate with Stryker’s storage server to store case data, audit/debug logs on the Stryker’s server. The 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 azure storage servers. The data is transmitted and stored in Azure cloud with the security and encryption as provided by the Azure cloud.

# PERSON AUTHENTICATION

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

During the case data upload to Stryker’s cloud, Knee Balancer application has the ability to authenticate the MPS user. This authentication is done via single sign on authentication mechanism. The user account which is logged into the Stryker’s device where the Knee Balancer app is installed can login into the application via single sign on feature. The authentication happens over the internet. The application communicates with Microsoft’s servers in order to authenticate the user via single sign on authentication mechanism.

However, while using the installed applications, the authentication is only by the device authentications set for iPhone/ IPad by the users.

# Password/ID Assignments

The Stryker admin must approve the installation of Knee Balancer application on the Stryker device. During data upload, the user can log in into the application via MSAL single sign on authentication mechanism. The application does not have ability to create/manage user account or password.

# User Account Management

The Knee Balancer application can be installed on the Stryker’s own iOS device from Stryker’s app store after approval from the Stryker’s admin. Once installed, application does not enforce any authorization mechanism to access the application.

For uploading data to cloud, the user can login into the application with single sign on authentication mechanism via MSAL authentication. The application communicates with MSAL servers to authenticate user into the application via single sign on. There is only single user who can access the application on a device. Thus, this section is not applicable. Users are requested to follow basic security hygiene to secure the iOS device:

* The device should get locked after left idle after reasonable period.
* Physical security should also be considered to manage access to the device.
* Application should not be installed on a non-Stryker device.

# PHYSICAL LOCKS

Note-This section is not applicable.

# ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE

Stryker follows the “Software Development Life Cycle” standard IEC 62304 as a part of development. Third party applications used within the product development are identified as SOUP items and are evaluated based on the risk categories.

# SOFTWARE BILL OF MATERIALS

# SBoM Structure and Updates

Knee Balancer application is a standalone application and does not require any other application to install or operate.

# SYSTEM AND APPLICATION HARDENING

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

# HEALTH DATA STORAGE CONFIDENTIALITY

The application does not collect or store any sensitive health data. This section is not applicable.

# TRANSMISSION CONFIDENTIALITY

Knee Balancer application transmits the data over the internet via API calls. The data created by user in the application will be transferred to the Stryker’s server/storage facilities. The data for storing in device and to transit does not contain any sensitive data such as patient information, credentials or certifications. However, the data is transmitted and stored in Azure cloud with the security and encryption as provided by the Azure cloud.

# TRANSMISSION INTEGRITY

The Knee Balancer application uploads case data to the Stryker’s cloud after the authentication through a secure HTTPS network. No PII or PHI is included in the data being transmitted to cloud. This data is only used for Post market complaints assessment.

# REMOTE SERVICE

Note-This section is not applicable.

# SECURITY PROGRAM INTEGRATION

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

# Vulnerability Management

Section 3.3, defines Stryker’s process for vulnerability identification, assessment, and communication. See Section 8, CYBER SECURITY PRODUCT UPGRADES, for information regarding software patches.

# Incident Response

Incident response will be per Product security post market management procedure at Stryker**.**

* ***Recommendation for*** ***MPS user:*** MPS user 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

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

* Do not connect to any unknown Wi-Fi network to gain access to internet.
* Device should be scanned on regular basis with anti-malware application for detection and mitigation of any threats and spywares
* Do not install any application from place other than Apple’s Appstore. Also, do not install unnecessary applications in the device.

# Risk Management

Stryker integrates cyber security risk management into its overall program for health and safety risk management. Both security and safety risk assessment were conducted for this device per guidelines in AAMI TIR57 and in compliance with EN/ISO 14971. Additionally, Stryker has a robust post market security risk management process which monitors the ongoing security posture of this device and addresses any security incidents that might arise.

# Training and Awareness

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

* Do not connect to any unknown Wi-Fi network to gain access to internet.
* Device should be scanned on regular basis with anti-malware application for detection and mitigation of any threats and spywares
* Do not install any application from place other than Apple’s Appstore. Also, do not install unnecessary applications in the device.
* 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.

# SECURE DECOMMISSIONING

***Recommendation for customer (MPS):*** Please reach out to Stryker Customer Care for secured decommissioning of Stryker owned Knee Balancer components such as (iOS device, tablets)*.* Components owned by MPS should follow the MPS IT policies for secure decommissioning.

# Appendix

# List of 3rd party components:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Title | Manufacturer | Version | Release Date | License Type | Maintenance procedure |
| MSAL (Microsoft Authentication libirary) | Microsoft | 1.2.2 | Jun-2022 | MIT | Not applicable |
| AZSClient (Azure Storage client library) | Microsoft | 0.2.6 | 01-Mar-2018 | MIT | Not applicable |
| MBProgressHUD | Matej Bukovinski | 1.2.0 | 13-Jan-2020 | MIT | Not applicable |