**[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 7](#_Toc112949890)

[3.1 Product and Manufacturer Identification 7](#_Toc112949891)

[3.2 Product Intended Use 7](#_Toc112949892)

[3.3 Related Manufacturer Programs 7](#_Toc112949893)

[3.4 System Characterization and System Assets 8](#_Toc112949894)

[3.5 System Security Context and Intended Environment 8](#_Toc112949895)

[3.6 Network, Data Flow Diagram 9](#_Toc112949896)

[4. MANAGEMENT OF PII and PHI 10](#_Toc112949897)

[5. AUTOMATIC LOGOFF 10](#_Toc112949898)

[6. AUDIT CONTROLS 10](#_Toc112949899)

[7. AUTHORIZATION 10](#_Toc112949900)

[8. CYBER SECURITY PRODUCT UPGRADES 11](#_Toc112949901)

[9. HEALTH DATA DE-IDENTIFICATION 11](#_Toc112949902)

[10. DATA BACKUP AND DISASTER RECOVERY 11](#_Toc112949903)

[11. EMERGENCY ACCESS 11](#_Toc112949904)

[12. HEALTH DATA INTEGRITY AND AUTHENTICITY 11](#_Toc112949905)

[13. MALWARE DETECTION/PROTECTION 11](#_Toc112949906)

[14. NODE AUTHENTICATION 12](#_Toc112949907)

[15. CONNECTIVITY CAPABILITIES 12](#_Toc112949908)

[15.1 Communication Provisions 12](#_Toc112949909)

[16. PERSON AUTHENTICATION 13](#_Toc112949910)

[17. PHYSICAL LOCKS 13](#_Toc112949911)

[18. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE 13](#_Toc112949912)

[19. SOFTWARE BILL OF MATERIALS 13](#_Toc112949913)

[20. SYSTEM AND APPLICATION HARDENING 13](#_Toc112949914)

[21. HEALTH DATA STORAGE CONFIDENTIALITY 14](#_Toc112949915)

[22. TRANSMISSION CONFIDENTIALITY 15](#_Toc112949916)

[23. TRANSMISSION INTEGRITY 15](#_Toc112949917)

[24. REMOTE SERVICE 15](#_Toc112949918)

[25. SECURITY PROGRAM INTEGRATION 15](#_Toc112949919)

[25.1 Vulnerability Management 15](#_Toc112949920)

[25.2 Incident Response 16](#_Toc112949921)

[25.3 Security Testing 17](#_Toc112949922)

[25.4 Scanning 17](#_Toc112949923)

[25.5 Risk Management 18](#_Toc112949924)

[25.6 Training and Awareness 18](#_Toc112949925)

[26. SECURE DECOMMISSIONING 18](#_Toc112949926)

[27. Appendix 20](#_Toc112949927)

[27.1 List of 3rd party components: 20](#_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

**AdvaMed** **- Advanced Medical Technology Association**: AdvaMed, or the Advanced Medical Technology Association, is an American medical device trade association, based in Washington, D.C. It is the largest medical device association in the world with U.S. and international members who are medical technology companies (medical devices, diagnostic products, and health information systems) that collectively represents 80% of U.S. medical technology firms in the United States, that produce close to 90% of annual health care technology purchases in the United States and more than 40% globally.

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

**Azure Cloud:** Azure cloud is used for archiving the logs and case input/output to the Azure blob storage once the exited from the case.

**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.

**Integrator**: The individual or organization who installs and configures the device/system into the operator’s environment.

**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).

**JSON format:** JSON (JavaScript Object Notation) is an open standard file format and data interchange format that uses human-readable text to store and transmit data objects consisting of attribute–value pairs and arrays (or other serializable values). It is a common data format with diverse uses in electronic data interchange.

**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.

**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). Refer-[www.nist.gov](http://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).

**OS – Operating System:** A mobile operating system is an operating system for mobile phones, tablets, smartwatches, 2-in-1 PCs, smart speakers, or other mobile devices.

**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.

**Shared Access Signature (SAS) Token:** A shared access signature (SAS) token provides secure delegated access to resources in your Azure storage account.

**SOM - Security Operations Manual**: A product-specific guide to the secure integration of a product into a customer IT network (this document).

**SSL certificate pinning:** SSL certificate pinning is a technique designed to prevent dangerous and complex security attacks. This security measure pins the identity of trustworthy certificates on mobile apps and blocks unknown documents from the suspicious servers.

**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.

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

# System Characterization and System Assets

Kneebalancer application is comprised of:

1. **iOS 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. **Azure Storage Server:** Azure cloud is used for archiving the logs and case input/output to the Azure blob storage once the exited from the case.

# System Security Context and Intended Environment



While there is no specific requirement for the Kneebalancer application to be fully functional other than a usual iOS environment, 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:

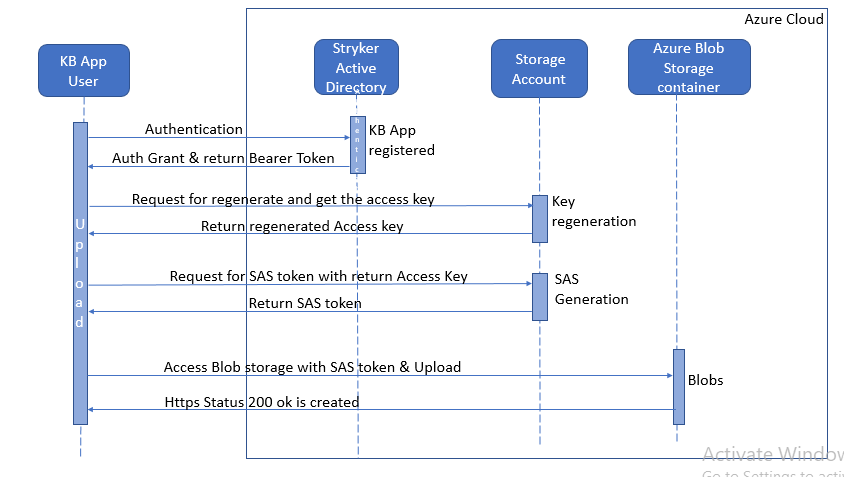
Devices operating in the intended use environment should consider that their IT infrastructure must obey different risk management approaches associated with their networks. Healthcare providers should adopt a risk management process adhering to general cybersecurity best practices to maintain the healthcare provider’s overall security status and their secure environment, as follows:

· Good physical security to prevent unauthorized physical access to device.  
· Access control measures (e.g., role based) to ensure only authenticated and authorized   
personnel are allowed access to network elements, stored information, services and   
applications.  
· General patch management practices that ensure timely security patch updates.

. Timely update of the devices and systems to prevent danger of using vulnerable software/OS  
· Malware protection to prevent unauthorized code execution.  
· 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 PII or PHI 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 HDO 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. Any other application installed on same device or user of the device does not have control over these logs.

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 ~~but are not restricted from doing the same.~~ The audit logs are uploaded along with case data and stored in Azure cloud with the security and encryption as provided by the Azure cloud. These logs are removed from the device within period of 30 days if not uploaded on storage server of Stryker. The logs are deleted from the device once they are uploaded to the cloud.

# AUTHORIZATION

~~Kneebalancer application can be installed via authorized entity of Stryker on the Stryker devices only. The installation of the Kneebalancer application from Stryker app store on the Stryker device must be approved by Stryker admin. Kneebalancer application does not enforce any authorization mechanism to access the Kneebalancer application as the mentioned earlier, the Kneebalancer application can be installed via authorized entity of Stryker only.~~

~~The Kneebalancer application does not have any role-based user access for the MPS users~~. A single user can upload case data created within Kneebalancer application on the Stryker’s storage server using Stryker’s credentials,

*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 at the MPS user’s site, a 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 azure storage server of Stryker. 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 personally identifiable information. Hence no option for the device user 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 doesn’t have any stored data on the device and other components. ~~The application does not contain any personally identifiable information. Hence no option for the device MPS MPS user user MPS user to access personally identifiable information.~~

# MALWARE DETECTION/PROTECTION

***Existing Security Features:***By default, the standalone Kneebalancer application does not have any malware detection features and requires the  *MPS* MPS 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:

***Recommendation for MPS users:***

* 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 app store. Moreover, install only required application on the device.
* Do not provide any unnecessary permissions (to access system component, data) to any other installed application.

# NODE AUTHENTICATION

Kneebalancer application does not to communicate with multiple devices, hence node authentication is required in the Kneebalancer application.

# CONNECTIVITY CAPABILITIES

The Kneebalancer application has the ability to connect to the network for the data transmission. No other connectivity capabilities such as removable media is required for the communication or any functioning of the application components.

# 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 storage server to store case data, audit/debug logs on the Stryker’s server. 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 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 Kneebalancer application via Stryker’s app store. Moreover, Stryker admin must approve the installation of the Kneebalancer application.

As the Kneebalancer application is installed on the secure device of the Stryker via secure channel, there is no authentication is required to access the application. However, Kneebalancer application has the authentication ability to authenticate single MPS user to upload the case data to the Stryker’s storage server. This authentication is done via Stryker’s credentials of the MPS user. The authentication happens over the network from the Stryker’s device where Kneebalancer application is installed.

# PHYSICAL LOCKS

Access to the Stryker’s device where Kneebalancer application is installed is only provided to Stryker MPS users and 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.

# 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.

# SOFTWARE BILL OF MATERIALS

~~The Kneebalancer application does not require software bill of materials. Hence, there is no provision of software bill of materials in the application.~~

# SYSTEM AND APPLICATION HARDENING

Systems hardening is a set of technologies, approaches, and best practices designed to reduce vulnerability in applications, systems, and other areas. Systems hardening aims to lower security risk by removing potential attack routes and reducing the attack surface of the system.

With the proper system hardening, attackers and malware agents have next to none opportunities to penetrate your IT environment by to gain a foothold within your IT ecosystem. Systems hardening demands a methodical approach to audit, identify, close, and control potential security vulnerabilities. The kind of hardening you implement relies on the risks associated with your current technology, the resources you have, and the importance of fixing problems. The essential ideas that are advised to be considered while putting the system hardening into practice are listed below:

* **Audit your existing systems:** Carry out a comprehensive audit of your existing technology. Use penetration testing, vulnerability scanning, configuration management, and other security auditing tools to find flaws in the system where the Kneebalancer application is installed and prioritize fixes.
* **Create a strategy for systems hardening:** You do not need to harden all of your systems at once. Instead, create a strategy and plan based on risks identified within your technology ecosystem, and use a phased approach to remediate the biggest flaws.
* **Patch vulnerabilities immediately:** Ensure that you have an automated and comprehensive vulnerability identification and patching system in place.
* **Network hardening:** Ensure your 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.
* **Operating system hardening:** Apply OS updates, service packs, and patches automatically; remove unnecessary drivers, file sharing, libraries, software, services, and functionality; encrypt local storage; tighten registry and other systems permissions; log all activity, errors, and warnings; implement privileged user controls.
* **Eliminate unnecessary accounts and privileges:** Enforce least privilege by removing unnecessary accounts (such as orphaned accounts and unused accounts) and privileges throughout your IT infrastructure.
* **Update system as well as other installed apps:** Configure Appstore to auto update third party and system apps as soon as update is available.
* **Network hardening:** Before connecting to any wireless network, ensure that wireless network is secure and is running on latest protocols. Also, do not connect to any public or open wireless network. It is also recommended to connect to trusted wireless networks only. Ensure your organization’s firewall is properly configured with all rules and is regularly audited.
* **Wireless interfaces hardening:** Along with the wireless network interface, other interfaces such as Bluetooth, RFID, NFC interfaces should be hardened. Configure best possible security mechanism such as connect only to Bluetooth version 3.0 devices, do not connect to external NFC devices automatically etc.

# 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. The Kneebalancer application uploads case data to the Azure storage server provided by Stryker after authentication via SAS token. SAS token is generated by using on application id. SAS token will expire within an hour. For every upload, a new SAS token must be generated, and this SAS token is not stored anywhere in the application or device.

Kneebalancer application transmits the data over the network via 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 Azure cloud. The SSL certificate pinning has been implemented in the application to further avoid any tampering of the data during transmission.

# TRANSMISSION INTEGRITY

The case data is uploaded to the Stryker’s cloud storage server of the Azure via API calls. The data is transmitted is encrypted with provision of SSL certificate. SSL pinning has been provided for additional transmission protection to prevent any man-in-the-middle attacks which can be performed by malicious actors.

# 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

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

# Incident Response

***Existing Security Features:***Only Stryker’s service engineer is authorized to visit & perform maintenance of the Kneebalancer 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 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 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 or latest hardware
* MPS user 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:**

* MPS user 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
* MPS user 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*** ***MPS user:*** MPS user’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 MPS user must block few IOCs and IOAs in their network devices. The MPS user is highly recommended to use the network firewall. Kneebalancer 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.

# 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 to communicate over the internet for authentication and data transfer. Hence, it is required for MPS user to have network level vulnerability scanning mechanism implemented. 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 WPA or WPS.
* Do not connect to any insecure wireless interfaces such as Bluetooth, NFC etc.
* 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

* MPS user 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

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 WPA or WPS 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.
* System should be updated on a regular basis and general anti-malware scanning should be performed.
* 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

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

# 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 |