This brochure contains information on the security and privacy controls that are part of the Reveal LINQ Mobile Manager System.


Cytoscape Overview

The Reveal LINQ Mobile Manager app uses AES encryption at the application layer. The Bluetooth link from the Patient Connector (Model 24965) to the tablet uses AES encryption for data storage and distance telemetry, hardening, proximity-based access control methods, and configuration management. The Reveal LINQ Mobile Manager app performs integrity checks and will shut down if tampering is detected. The Reveal LINQ Mobile Manager app also checks for potential insecure mobile device configurations and shuts down if unsafe conditions are detected in the tablet. It uses advanced obfuscation techniques like white box cryptography to protect encryption keys during handling.

The app resides in a secure container on the tablet. This technique is also known as “app sandboxing,” a security feature in the iOS and Android® operating systems (OS). The Reveal LINQ Mobile Manager app also benefits from other OS security features like Address Space Layout Randomization (ASLR), non-executable memory, and application code signing.

The integrity of the Reveal LINQ Mobile Manager is also maintained through digital signature validation of all software loaded on the Patient Connector. Additionally, the integrity and authenticity of the Reveal LINQ Mobile Manager app is verified through a self-check during startup and periodically thereafter.

The Reveal LINQ Mobile Manager was designed to be at least 95% successful in patient data transmission to the CareLink network when the tablet has reliable Internet connectivity. Because patient data handled by the Reveal LINQ Mobile Manager is not needed or reviewed by clinicians in real-time, the Reveal LINQ Mobile Manager app will keep trying to transfer the data to the CareLink network until successful or until 7 days elapse. This mitigates against patient data loss due to reductions or outages in the cellular network, Wi-Fi network, or the CareLink network.

Access controls are also in place for the Reveal LINQ Mobile Manager’s network communications. The CareLink network authenticates the Reveal LINQ Mobile Manager prior to allowing connections. The Reveal LINQ Mobile Manager uses certificate pinning to validate the identity of the CareLink network before establishing a connection.

The Reveal LINQ Mobile Manager app utilizes a “something you have” authentication factor using the Patient Connector to control user access to its features. Some features like device registration require user authentication.

Proximity control using inductive telemetry mitigates against unauthorized access to the Reveal LINQ ICM via the Reveal LINQ Mobile Manager.

To prevent unauthorized access to the tablet used for the Reveal LINQ Mobile Manager, use the key card to enable encryption and passcode- or biometrics-based authentication on the tablet.

ACCOUNTABILITY

Each Patient Connector has a unique serial number and network credentials. These items are used to uniquely identify each Patient Connector when it’s used to connect to the CareLink network. Each Reveal LINQ Mobile Manager app installation has an ID that is used to uniquely identify the app when it interacts with the CareLink network.

SUMMARY

The Reveal LINQ Mobile Manager’s secure design and development began with a preliminary risk analysis and threat model that considered safety and cybersecurity risks. The identified risks were then used to generate the security design input requirements that continue to be updated as new vulnerabilities and threats are discovered in technologies utilized in, and interfaced by the Reveal LINQ Mobile Manager. The requirements have led to a strong security architecture that has been tested and reviewed, both internally and externally. Security design controls like mobile application hardening, proximity-based access control methods, AES encryption for data storage and distance telemetry, and TLS-based secure communications were implemented to reduce security risks. The security design controls have effectively reduced security and patient safety risks to the lowest rate.

The Reveal LINQ Mobile Manager is only compatible with the Patient Connector paired with the Reveal LINQ Mobile Manager app through a passkey pairing method using a secure code distributed with the patient’s insertable cardiac monitor, which is a diagnostic and monitoring device not capable of delivering therapy. The Reveal LINQ Mobile Manager handles Protected Health Information (PHI) but is considered low-risk since the PHI does not include health insurance, billing, and prescription information. Extra precautions have been taken to ensure that the patient data is retained in the Reveal LINQ Mobile Manager app for the shortest possible period.

During transmission of patient data from the Reveal LINQ Mobile Manager app to the CareLink network, the data is protected by a Transport Layer Security (TLS) network connection and encrypted with AES. In the event that the Reveal LINQ Mobile Manager app is unable to complete the transmission to the CareLink network, the Reveal LINQ Mobile Manager app will keep trying to transfer the data to the CareLink network for a maximum of 7 days. The Reveal LINQ Mobile Manager app will then delete the patient data.

The Reveal LINQ Mobile Manager app uses AES encryption to protect its credentials including encryption keys and tokens. It does not persist any user passwords.

AUTHENTICATION AND AUTHORIZATION

Secure Bluetooth pairing is the access control mechanism for the Reveal LINQ Mobile Manager’s Bluetooth communications. This pairing ensures that the Reveal LINQ Mobile Manager app only communicates with authorized Medtronic Patient Connectors, and vice versa.

The Cardiac Rhythm and Heart Failure business unit of Medtronic has implemented the following secure design practices for all products:

- Risk identification and mitigation
- Security-related stakeholder needs elicitation
- Design input requirements engineering
- Secure design controls
- Traceability
- Secure implementation
- Verification and validation

These practices are meant to ensure security considerations for all design solutions in development, and to provide a method to quickly address newly discovered security vulnerabilities and threats to products already placed on the market.

Medtronic identifies security risks and tests the corresponding mitigations throughout the development process. External third-party penetration testing, vulnerability assessments, and secure code reviews are also standard practice during the development and final production readiness phases.

The following information addresses the security principles identified in the Food and Drug Administration (FDA) guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, 2 Oct 2014, as well as best practices in information security and design.

SECURITY OF DATA

Medtronic followed a secure design lifecycle approach in ensuring the confidentiality, integrity, and availability (CIA) of the Reveal LINQ Mobile Manager’s information assets.

CONFIDENTIALITY

Encryption and proximity control are used to ensure confidentiality of data. Advanced Encryption Standard (AES) is used to protect all patient data while it is in a state of transit or storage in the Reveal LINQ Mobile Manager app.

INTENSITY

The Reveal LINQ Mobile Manager app has implemented mobile application hardening techniques like binary and run-time protections. The Reveal LINQ Mobile Manager app performs integrity checks and will shut down if tampering is detected. The Reveal LINQ Mobile Manager app also checks for potentially insecure mobile device configurations and shuts down if unsafe conditions are detected in the tablet. It uses advanced obfuscation techniques like white box cryptography to protect encryption keys during handling.

The app resides in a secure container on the tablet. This technique is also known as “app sandboxing,” a security feature in the iOS and Android® operating systems (OS). The Reveal LINQ Mobile Manager app also benefits from other OS security features like Address Space Layout Randomization (ASLR), non-executable memory, and application code signing.

The integrity of the Reveal LINQ Mobile Manager is also maintained through digital signature validation of all software loaded on the Patient Connector. Additionally, the integrity and authenticity of the Reveal LINQ Mobile Manager app is verified through a self-check during startup and periodically thereafter.

The Reveal LINQ Mobile Manager was designed to be at least 95% successful in patient data transmission to the CareLink network when the tablet has reliable Internet connectivity. Because patient data handled by the Reveal LINQ Mobile Manager is not needed or reviewed by clinicians in real-time, the Reveal LINQ Mobile Manager app will keep trying to transfer the data to the CareLink network until successful or until 7 days elapse. This mitigates against patient data loss due to reductions or outages in the cellular network, Wi-Fi network, or the CareLink network.

AUTHENTICATION AND AUTHORIZATION

Secure Bluetooth pairing is the access control mechanism for the Reveal LINQ Mobile Manager’s Bluetooth communications. This pairing ensures that the Reveal LINQ Mobile Manager app only communicates with authorized Medtronic Patient Connectors, and vice versa.

Access controls are also in place for the Reveal LINQ Mobile Manager’s network communications. The CareLink network authenticates the Reveal LINQ Mobile Manager prior to allowing connections. The Reveal LINQ Mobile Manager uses certificate pinning to validate the identity of the CareLink network before establishing a connection.

The Reveal LINQ Mobile Manager app utilizes a “something you have” authentication factor using the Patient Connector to control user access to its features. Some features like device registration require user authentication.

Proximity control using inductive telemetry mitigates against unauthorized access to the Reveal LINQ ICM via the Reveal LINQ Mobile Manager.

To prevent unauthorized access to the tablet used for the Reveal LINQ Mobile Manager, use the key card to enable encryption and passcode- or biometrics-based authentication on the tablet.

ACCOUNTABILITY

Each Patient Connector has a unique serial number and network credentials. These items are used to uniquely identify each Patient Connector when it’s used to connect to the CareLink network. Each Reveal LINQ Mobile Manager app installation has an ID that is used to uniquely identify the app when it interacts with the CareLink network.

SUMMARY

The Reveal LINQ Mobile Manager’s secure design and development began with a preliminary risk analysis and threat model that considered safety and cybersecurity risks. The identified risks were then used to generate the security design input requirements that continue to be updated as new vulnerabilities and threats are discovered in technologies utilized in, and interfaced by the Reveal LINQ Mobile Manager. The requirements have led to a strong security architecture that has been tested and reviewed, both internally and externally. Security design controls like mobile application hardening, proximity-based access control methods, AES encryption for data storage and distance telemetry, and TLS-based secure communications were implemented to reduce security risks. The security design controls have effectively reduced security and patient safety risks to the lowest rate.
Reveal LINQ™ Insertable Cardiac Monitor, Reveal LINQ™ Mobile Manager System

Indications: The Reveal LINQ™ insertable cardiac monitor (ICM) is an implantable patient-activated and automatically-activated monitoring system that records subcutaneous ECG and is indicated in the following cases:

- Patients with clinical syndromes or situations at increased risk of cardiac arrhythmias
- Patients who experience transient symptoms such as dizziness, palpitation, syncope, and chest pain, that may suggest a cardiac arrhythmia

Caution: The device is intended for use in patients who are not able to communicate their medical history or are unable to activate the device autonomously.

Usage: The device is designed for continuous monitoring of cardiac rhythm, detecting and recording arrhythmias, and providing alerts for potential issues.

Battery Life: The device is powered by a rechargeable battery, and the average battery life is 3 years. Users are advised to charge the device periodically.

Environmental Precautions: The device is susceptible to electromagnetic interference and should not be used near devices that generate such interference, such as microwave ovens or radios.

Safety: The device is strong and durable, but users are advised to avoid physical trauma to the device.

Medtronic MyCareLink™ Patient Monitor, Medtronic CareLink™ Network, and CareLink™ Mobile Application

Intended Use: The Medtronic MyCareLink™ patient monitor and CareLink™ network are intended for use in the transfer of patient data from Medtronic implantable cardiac devices. The CareLink™ mobile application is intended to provide current CareLink network customers access to CareLink network data via a mobile device for their convenience. The CareLink™ mobile application is not a substitute for appropriate medical attention in the event of an emergency and should only be used as directed by a physician.

Potential Complications: Potential complications of the Reveal LINQ™ device include, but are not limited to, device rejection phenomena (including local tissue reaction), device migration, infection, and erosion through the skin.

Contraindications: There are no known contraindications for the use of the Reveal LINQ™ ICM. However, the patient should be informed of the risks and benefits of the procedure.

Warnings and Precautions: The patient should be informed of the risks and benefits of the procedure.

Radiofrequency (RF) interference — Portable and mobile RF communications equipment can interfere with the operation of the patient connector. There is no guarantee that the device will not receive interference or that the interference will not affect device performance. To avoid interference, do not use the patient connector near other wireless communications equipment.

Environmental precautions — To ensure safe and effective operation, use the device with care to avoid damage to the patient connector. Environmental factors that may impact the function of the device include: heat, moisture, mechanical stress, and electromagnetic interference. The device is designed to be resistant to these factors, but users are advised to take precautions to ensure safe operation.

Important Reminder: This information is intended only for users in markets where Medtronic products and therapies are approved or available for use as indicated within the respective product manuals. Content on specific Medtronic products and therapies is not intended for users in markets that do not have authorization for use.