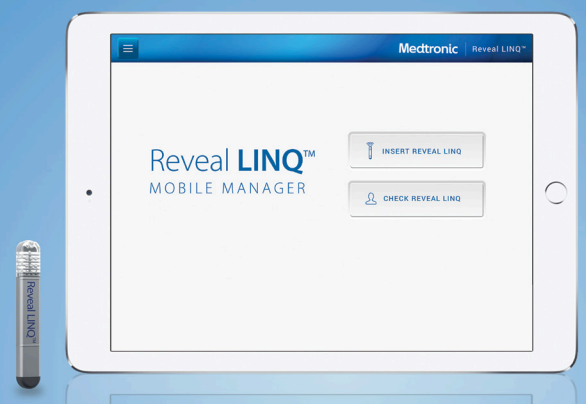
SECURITY PROGRAM

Reveal LINQ™ Mobile Manager



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

Medtronic

CYBERSECURITY INTRODUCTION

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.

Proximity control using inductive telemetry protects the confidentiality of the information exchanged between the Patient Connector and the insertable device.

The **Bluetooth**® link from the Patient Connector (Model 24965) to the tablet uses AES encryption at the application layer.

The Medtronic Patient Connector needs to be paired to the Reveal LINQ Mobile Manager app via Bluetooth. At any given time, the Reveal LINQ Mobile Manager app can only communicate with one Patient Connector. Application layer encryption was implemented as a defense-in-depth strategy to ensure confidentiality of information even if future vulnerabilities and limitations are discovered in the Bluetooth protocols. The Patient Connector is paired with the Reveal LINQ Mobile Manager app through a passkey pairing method using a secure code distributed with the clinician Patient Connector. The Patient Connector encrypts the patient's insertable device data before transmitting it to the Reveal LINQ Mobile Manager app. The Reveal LINQ Mobile Manager is only compatible with the Reveal LINQ insertable cardiac monitor, which is a diagnostic and monitoring device that is not capable of delivering therapy. The Reveal LINQ Mobile Manager handles Protected Health Information (PHI) but it 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.

INTEGRITY

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.

AVAILABILITY

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 clinician users 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, the user is advised 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. Also, 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 Mobil 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.

Indications, Safety, and Warnings

If you are located in the United States, please refer to the brief statement below to review applicable indications, safety, and warning information. See the device manual for detailed information regarding the implant procedure, indications, contraindications, warnings, precautions, and potential complications/adverse events. For further information, please call Medtronic at 763-514-4000 and/or consult the Medtronic website at medtronic.com.

If you are located outside the United States, see the device manual for detailed information regarding instructions for use, the implant procedure, indications, contraindications, warnings, precautions, and potential adverse events. If using an MRI SureScan™ device, see the MRI SureScan technical manual before performing an MRI. For further information, contact your local Medtronic representative and/or consult the Medtronic website at medtronic.com.

www.medtronic.com/manuals

Consult instructions for use at this website. Manuals can be viewed using a current version of any major Internet browser. For best results, use Adobe Acrobat Reader ®with the browser.

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.

The Medtronic MyCareLink patient monitor and the Medtronic CareLink network are indicated for use in the transfer of patient data from Medtronic implantable cardiac devices. These products are not a substitute for appropriate medical attention in the event of an emergency. Data availability and alert notifications are subject to Internet connectivity and access, and service availability. The MyCareLink patient monitor must be on and in range of the device. Alert notifications are not intended to be used as the sole basis for making decisions about patient medical care.

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

The device has not been tested specifically for pediatric use.
Reveal LINQ Mobile Manager System: The Reveal LINQ Mobile Manager app is intended for programming and interrogating the Reveal LINQ ICM LNQ11. The Medtronic patient connector is a portable electronic device using low frequency inductive telemetry to communicate with the Reveal LINQ ICM. The patient connector uses Bluetooth® technology to transmit implantable heart device data to the Reveal LINQ Mobile Manager app for further processing. The patient connector is intended to be used by healthcare personnel only in a clinical or hospital environment. **Patient Assistant:** The Patient Assistant is intended for unsupervised patient use away from a hospital or clinic. The Patient Assistant activates the data management feature in the Reveal™ insertable cardiac monitor to initiate recording of cardiac event data in the implanted device memory.
Contraindications: There are no known contraindications for the implant of the Reveal LINQ ICM or for the Reveal LINQ Mobile Manager system. However, the patient's particular medical condition may dictate whether or not a subcutaneous, chronically implanted device can be tolerated.
Reveal LINQ Insertable Cardiac Monitor
Warnings/Precautions: Patients with the Reveal LINQ ICM should avoid sources of diathermy, high sources of radiation, electrosurgical cautery, external defibrillation, lithotripsy, therapeutic ultrasound, and radiofrequency ablation to avoid electrical reset of the device, and/or inappropriate sensing as described in the Medical procedure and EMI precautions manual. MRI scans should be performed only in a specified MR environment under specified conditions as described in the Reveal LINQ MRI Technical Manual.
Reveal LINQ Mobile Manager System: Before inserting the Reveal LINQ ICM, verify that the patient connector and mobile device are fully charged. The patient connector and mobile device may run out of power during the insertion procedure if they are not fully charged. You will not be able to program or interrogate the patient's Reveal LINQ ICM until the patient connector and the mobile device have power.

Only use the patient connector to communicate with the intended implanted device. Do not use the patient connector to communicate with other implanted devices. Using the patient connector to communicate with other implanted devices can interfere with those devices, potentially affecting the other implanted device's functionality or therapy delivery.

Use of wireless devices — The patient connector incorporates radiofrequency (RF) communications components which may affect other devices and equipment in the medical environment. The use of wireless devices in the medical environment must be evaluated and authorized by the responsible organization. RF interference may affect device performance. Electromagnetic Compliance (EMC) testing shows that the patient connector provides reasonable protection against harmful interference and provides EMC immunity in a typical medical installation. The use of wireless devices in the medical environment must be evaluated and authorized by the responsible organization. However, there is no guarantee that interference will not occur in a particular installation. If the patient connector does cause harmful interference to other devices or is negatively impacted by other devices, correct the interference by one or more of the following measures: reorient or relocate the patient connector and other devices; increase the separation between the patient connector and other devices by at least two meters (approximately 6 feet); and/or turn off any interfering equipment.

Radiofrequency (RF) interference — Portable and mobile RF communications equipment can interfere with the operation of the patient connector. There is no guarantee that it will not receive interference or that any particular transmission from this system will be free from interference. To avoid interference, do not use the patient connector and mobile device within 2 m (6 feet) of other wireless communications equipment. Using the patient connector near these devices could interfere with communication between the Reveal LINQ ICM and the patient connector.
Security — Maintain adequate physical security of the patient connector to prevent unauthorized use that could lead to harm to patients. Bluetooth communication in the patient connector is encrypted for security. Medtronic inductive telemetry uses short-range communication to protect patient information. If the patient connector should fail, there is no risk of patient harm.

Environmental precautions — To ensure safe and effective operation, use the device with care to avoid damage to the patient connector from environmental factors that may impair its function. Care is exercised in design and manufacturing to minimize damage to devices under normal use. However, electronic devices are susceptible to many environmental stresses. Specifically, the patient connector may be affected by electrostatic discharge (ESD). In an environment likely to cause ESD, such as a carpeted floor, discharge any charge collected on your body before touching the device.

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.

Medtronic MyCareLink™ Patient Monitor, Medtronic CareLink™ Network, and CareLink™ Mobile Application
Intended Use: The Medtronic MyCareLink patient monitor and CareLink network are indicated for use in the transfer of patient data from some Medtronic implantable cardiac devices based on physician instructions and as described in the product manual. 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 replacing the full workstation, but can be used to review patient data when a physician does not have access to a workstation. These products are not a substitute for appropriate medical attention in the event of an emergency and should only be used as directed by a physician. CareLink network availability and mobile device accessibility may be unavailable at times due to maintenance or updates, or due to coverage being unavailable in your area. Mobile device access to the Internet is required and subject to coverage availability. Standard text message rates apply.

Contraindications: There are no known contraindications.

Warnings and Precautions: The MyCareLink patient monitor must only be used for interrogating compatible Medtronic implantable devices.

See the device manuals for detailed information regarding the implant procedure, indications, contraindications, warnings, precautions, and potential complications/adverse events. For further information, please call Medtronic at 1-800-328-2518 and/or consult the Medtronic website at medtronic.com.

Caution: Federal law (USA) restricts these devices to sale by or on the order of a physician.

Medtronic
710 Medtronic Parkway
Minneapolis, MN 55432-5604
USA

Toll-free in USA: 800.633.8766
Worldwide: +1.763.514.4000

medtronic.com

UC201605574a EN ©2017 Medtronic.
Minneapolis, MN. All Rights Reserved.
Printed in USA. 10/2017

Medtronic