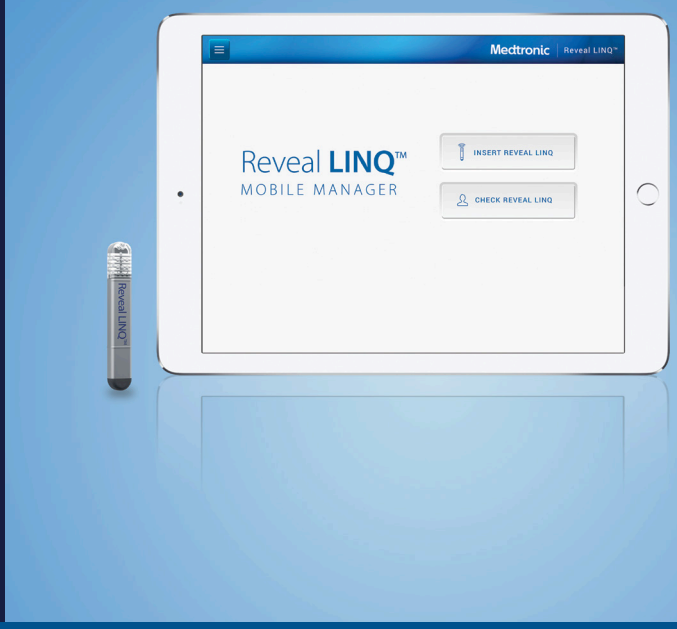
SECURITY PROGRAM

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 theinsertable 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 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.

Brief Statement
See the device manual for detailed information regarding the instructions for use, the implant procedure, indications, contraindications, warnings, precautions, and potential adverse events. For further information, contact your local Medtronic representative 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.

Europe
Medtronic International Trading Sàrl.
Route du Molliau 31
Case postale
CH-1131 Tolochenaz
www.medtronic.eu
Tel: +41 0 21 802 70 00
Fax: +41 0 21 802 79 00

United Kingdom/Ireland
Medtronic Limited
Building 9
Croxley Green Business Park
Hatters Lane
Watford
Herts WD18 8WW
www.medtronic.co.uk
Tel: +44 0 1923 212213
Fax: +44 0 1923 241004

medtronic.eu

Medtronic