CARELINK SMARTSYNC™ DEVICE MANAGER SECURITY WHITE PAPER

CareLink SmartSync™ Device Manager Security

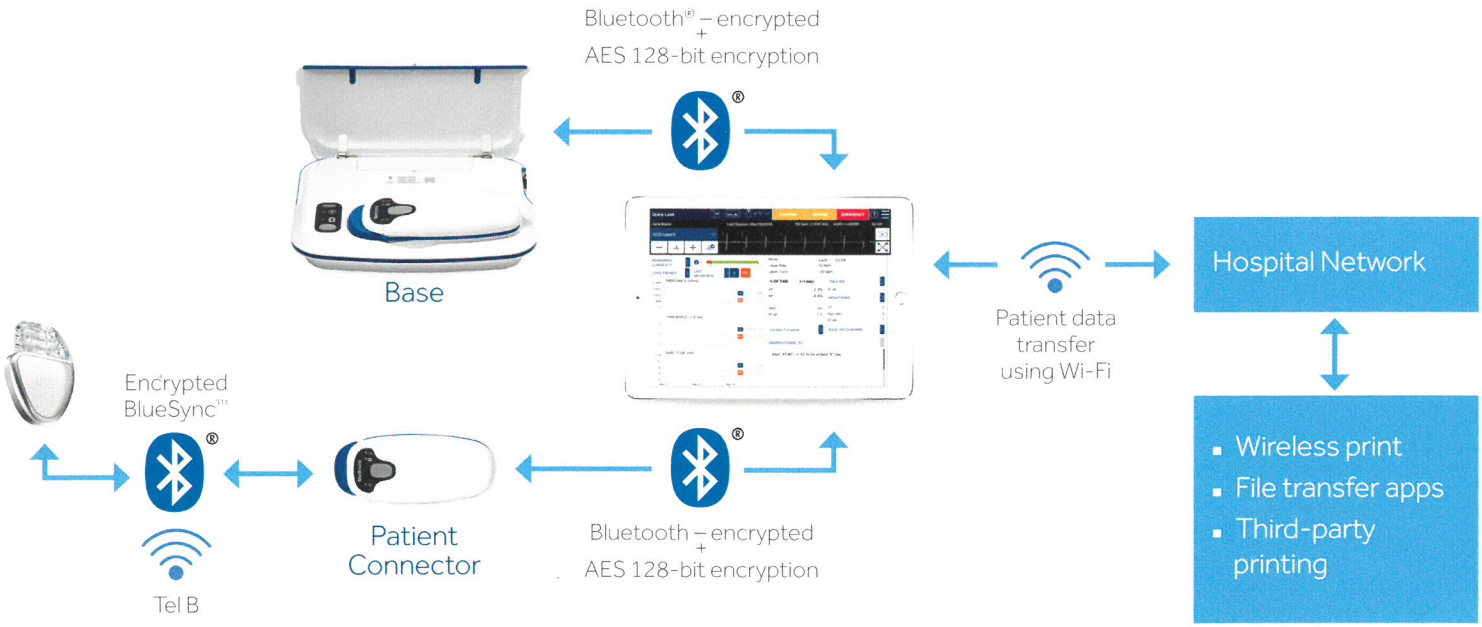
CareLink SmartSync Device Manager is the Medtronic next-generation programmer that securely communicates with Medtronic cardiac implantable electronic devices (CIED) and provides pacing lead analyzer (PSA) functions. The CareLink SmartSync Device Manager consists of a Base (24970A), Patient Connector (24967), and the SmartSync application (app) installed on a mobile device (tablet). SmartSync is used by healthcare providers and Medtronic representatives in a clinical or hospital environment to securely communicate with Medtronic CIEDs and the PSA to conduct lead analysis and CIED implant and follow-up procedures. The SmartSync app has been designed to secure all communication paths, to secure data at rest, and to secure its software and hardware components. Medtronic has integrated security design into all aspects of CareLink SmartSync Device Manager development.

This white paper details the security features of the CareLink SmartSync Device Manager.

Healthcare Professional Summary

Clinical Workflow

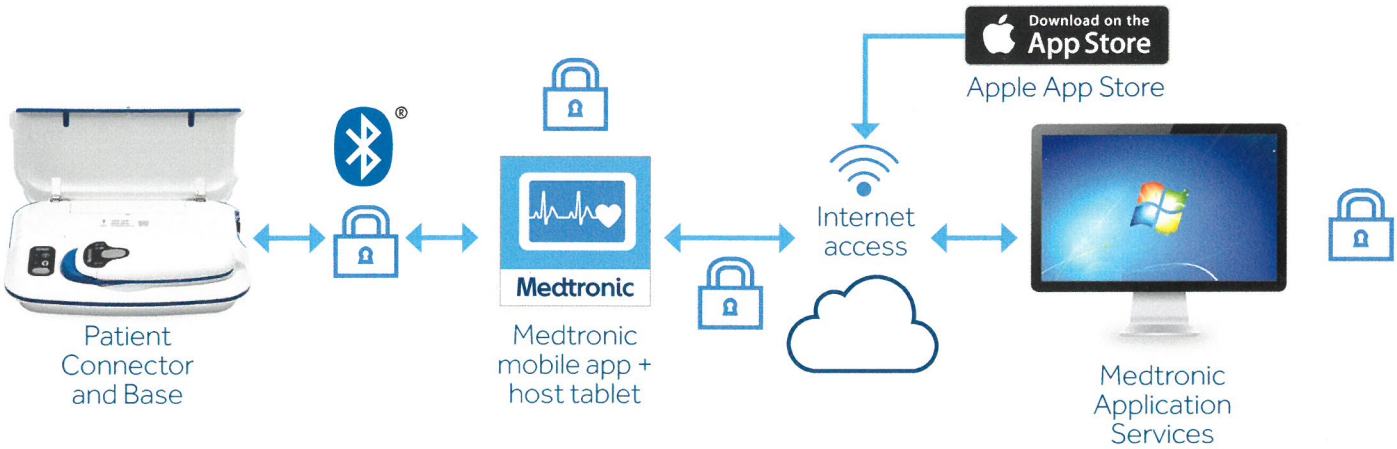
The SmartSync app connects with the Base to utilize ECG, EGM, and PSA during CIED implant or follow-up procedure. The SmartSync app connects with the Patient Connector to communicate with the CIED during programming and interrogation. Patient data interrogated from the CIED is stored within the SmartSync app and can be exported to the hospital network. The SmartSync app does not interface with Medtronic CareLink™ network.



Medtronic

Support Workflow

The CareLink SmartSync Device Manager support strategy includes regular software and firmware updates to ensure security, reliability, and the latest CIED support capabilities. The SmartSync app is downloaded and updated from the Apple App Store®. The app receives content updates from Medtronic Application Services (MAS). The content received from MAS includes CIED app support definition, Base and Patient Connector firmware, End User License Agreement (EULA), and help. Additionally, the SmartSync app sends debug logs to MAS to assist Medtronic technical support in troubleshooting issues. The debug logs only contain app, Patient Connector, and Base debug information. No patient information or CIED data is included in log files. No patient information or CIED data is sent to MAS.



Security Controls

CareLink SmartSync Device Manager was designed with security controls in place to protect communications, patient data, and CIED data. The system includes the following controls:

- Encrypted paired communications is used between Base, Patient Connector, and the SmartSync app. Physical interaction with the Base or Patient Connector is required to establish the paired communication with the SmartSync app.
- Data on the CareLink SmartSync Device Manager tablet is encrypted with 256-bit AES application level encryption as well as mobile OS file system encryption.
- PIN enforcement on the tablet ensures the strongest level of file system encryption.
- The SmartSync app on the tablet is protected using tamper-detection, rooted kernel detection, and integrity checks to ensure the application has not been tampered with and is operating as expected.
- The SmartSync app establishes an encrypted communication connection between the SmartSync app and MAS on all Wi-Fi or cellular connections. Data and commands are protected over secure communication connections.
- SmartSync app does not send patient data to Medtronic Application Services (MAS). Debug logs without patient data are sent to MAS and application updates are received from MAS.
- MAS requires physical possession of either a Base or Patient Connector to establish and authenticate a connection with the SmartSync app.
- Medtronic-provided tablets are controlled and managed by Intelligent Hub Mobile Device Manager (MDM) software. Users providing their own tablets are responsible for managing tablet settings according to their IT policies.
- The SmartSync app does NOT connect to the CareLink network.

Secure Development Practices

The CareLink SmartSync Device Manager has been comprehensively tested for security. In addition to extensive Medtronic testing, Medtronic has engaged specialized security testing experts to perform third party testing and perform secure design reviews. Medtronic ensures secure Software Development Life Cycle (SDLC) practices are followed and ongoing monitoring of threat intelligence and cyber security vulnerabilities are managed. These secure development practices provide confidentiality, integrity, and availability.

Confidentiality

To ensure confidentiality of data, encryption is used at each point where patient data could be accessed, if intercepted by a third party. The physical communication transport layers and the data layer (Patient data package) are separately encrypted using different encryption methods. The Bluetooth link between the Base/Patient Connector and the SmartSync app uses standard Bluetooth encryption.

During a PSA or CIED session, the Base or Patient Connector is one-to-one paired to the SmartSync app through standard implementation of data layer level encryption. This was implemented to reduce risk posed from security limitations in the Bluetooth protocol. In addition, the CareLink SmartSync Device Manager hardware is one-to-one paired with the SmartSync app using an out of band security key distributed with the CareLink SmartSync hardware. The Base and/or Patient Connector encrypts data before transmitting it to the SmartSync app hosted on the tablet. Patient data obtained during a PSA or CIED session is retained in the SmartSync app and automatically deleted after a period of time set by the user; the default setting is seven days. Patient data can be manually deleted by the user at any time.

Communications between SmartSync and MAS are for software updates or debug log collection. No patient data is sent or received by MAS. All communications with MAS are encrypted.

Integrity

The integrity of CareLink SmartSync Device Manager is maintained through verification of all installed software. Additionally, the application is verified through a self-check every time an application is started. All software installed on the Base/Patient Connector during manufacturing and through in-field updates has a cryptographic signature. This signature is traceable back to the Medtronic Root Certificate which is located and stored within a Hardware Security Module (HSM) and adheres to strict chain-of-custody practices. During installation, this signature is verified for each software item being installed. If the software does not match the expected signed certificate, then the software is not installed.

The Base/Patient Connector will not accept communication requests from the SmartSync app until after successful security key pairing with the application. In addition, only valid communication requests associated with the SmartSync app will be accepted by the Base/Patient Connector. If the security key exchange fails, the session will be ended immediately. Additionally, message integrity checks are included in the Bluetooth messages to ensure messages and commands are intact and have not been altered.

The SmartSync app is signed and verified using a protected Medtronic signature and operates in a secured partition on the tablet. This ensures only valid tablet inputs are addressed by the application. The secured partition also ensures the tablet RAM and other tablet resources are not shared with other non-CareLink SmartSync Device Manager applications.

Availability

The CareLink SmartSync Device Manager has been designed to be available to support lead analysis and CIED implant and follow-up procedures with 100% availability. An internet connection is not required to perform a PSA or CIED patient session. Internet connection is only required to export patient session reports/data, to obtain software, and send debug logs to MAS.

Customer Security Considerations

The CareLink Smart Sync Device Manager has followed a design for security process to maintain integrity of the Medtronic components and data. Data is secure and protected while residing inside the SmartSync app. Users should be aware that data exported from the SmartSync app should be protected in accordance with local policy for protecting data in transit. Local policy for using and protecting data outside of the controlled application container should be followed to ensure compliance with local security and privacy policies and practices.