BLUESYNC™ TECHNOLOGY SECURITY WHITE PAPER

BlueSync™ Technology Security

BlueSync Technology leverages secure technology to wirelessly connect patients and their cardiac devices to clinicians for data access, tracking, and management. As the adoption of medical devices connecting with patient cell phones and tablets increases, questions around patient and data security have come to the forefront. Medtronic integrates strong security design into its product development process and monitors for potential security vulnerabilities after products are released. The BlueSync technology platform introduces innovative features with robust security to protect the device and patient data. This whitepaper details the security features of the BlueSync technology remote monitoring system.

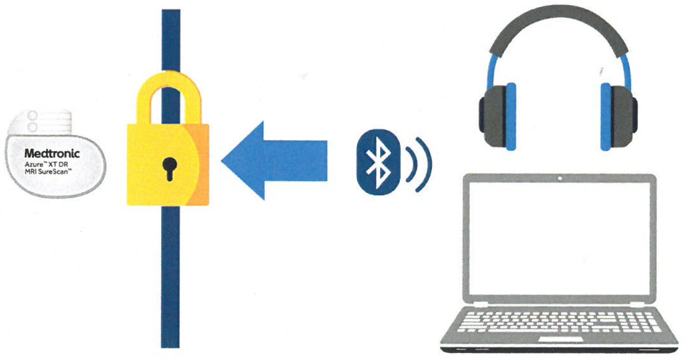
Heathcare Professional Summary

The Azure™ and Percepta™ family of pacemakers introduce BlueSync technology with Bluetooth® Low Energy for remote monitoring through the CareLink™ Network. Security for the BlueSync technology was designed to protect the device, patient data, and connectivity. These security features include:

- Cardiac device cannot be programmed remotely. Programming of the device is only possible if the patient is in the hospital or clinic and in very close proximity to the programming head of a Medtronic device programmer.
- Device battery life is protected with controls that temporarily shut down the Bluetooth interface if Bluetooth Low Energy communication is initiated from other than the CareLink network. This prevents hackers from trying to drain battery with repeated communication attempts. The Bluetooth interface is re-enabled if the cardiac device has an alert condition to relay to CareLink.
- Device data is encrypted. Data collected by the cardiac device is encrypted before sending it to the CareLink network through the Bluetooth patient monitor (MyCareLink™ monitor or patient-owned mobile platform*). This encryption means that the Bluetooth monitor acts as a passthrough and cannot read the data or make unauthorized changes to pacemaker therapy settings.
- Each cardiac device is given a unique encryption key. Only the device with that unique key will respond to the commands from the CareLink Network.
- Remote monitoring through Bluetooth Low Energy can be disabled by the physician programmer if patients have concerns about monitoring via Bluetooth.

Security Details

Implanted medical devices have used distance radio communication for more than a decade and utilize proprietary communication protocols in dedicated frequency bands. Medtronic BlueSync heart devices provides the capability of remote monitoring through Bluetooth Low Energy.



Medtronic

Security Details, *continued*

Medtronic has implemented a variety of security controls for the Bluetooth Low Energy interfaces for cardiac devices with BlueSync technology.

Limited Commands: Over Bluetooth Low Energy, cardiac devices with BlueSync technology only accept remote monitoring commands. Changes to therapy settings are not accepted through patient-owned mobile platform* or patient monitor.

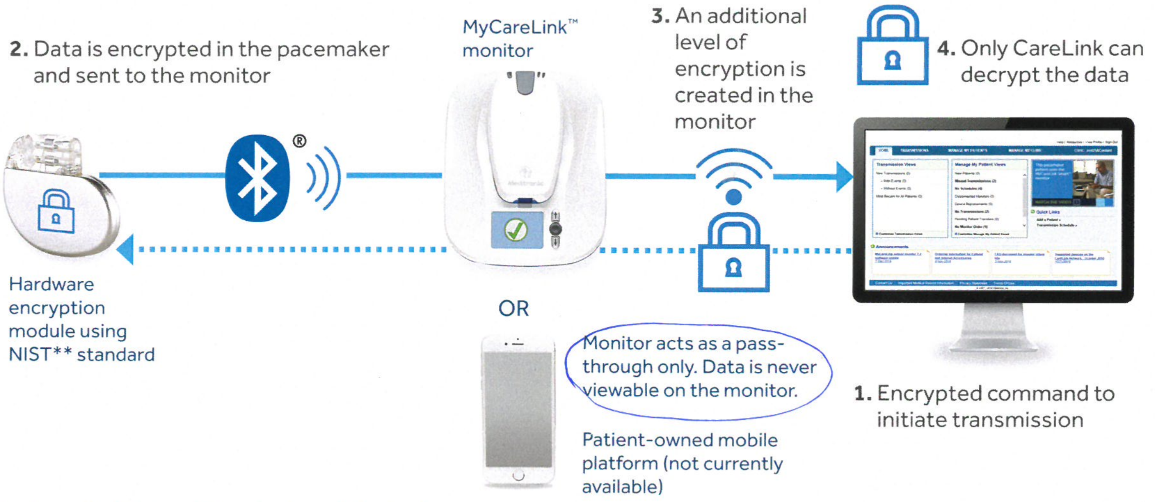
Battery Protection: Our device longevity models include the impact of using Bluetooth Low Energy for remote monitoring. To manage the longevity impact, we control the amount of telemetry that can be used.

- Connections to non-Medtronic devices or apps are rejected by the pacemaker. After multiple communication attempts from non-Medtronic devices in a given day, the Bluetooth Low Energy radio is disabled for the rest of the day.
- The total duration of daily Bluetooth Low Energy communication is limited. After the limit is reached, the Bluetooth Low Energy radio is disabled for the rest of the day.

Medtronic programmers can establish communication with the cardiac device even if the Bluetooth Low Energy interface is disabled allowing device interactions for emergency care or other clinic device follow-ups. The device will also re-enable the Bluetooth Low Energy radio if it has a CareAlert™ to communicate.

End-to-end encryption: Encryption keys are created uniquely for each cardiac device with BlueSync technology and additional keys are created for the communication with the CareLink Network ensuring the device can only communicate with the CareLink network. The cardiac device encrypts device data prior to sending it to Medtronic remote monitoring platforms over the Bluetooth Low Energy interface. A message integrity check is included in the message to ensure the message or command is intact and has not been altered.

encryption + auth.


2. Data is encrypted in the pacemaker and sent to the monitor
MyCareLink™ monitor
3. An additional level of encryption is created in the monitor
4. Only CareLink can decrypt the data
Hardware encryption module using NIST** standard
OR
Monitor acts as a pass-through only. Data is never viewable on the monitor.
Patient-owned mobile platform (not currently available)
1. Encrypted command to initiate transmission

**NIST: National Institute of Standards and Technology

External Testing

The Azure pacemaker, the Bluetooth patient monitors, and the CareLink Network functions for the Azure pacemaker have been comprehensively tested for security. In addition to Medtronic's extensive internal testing, Medtronic engaged outside security researchers to assess potential security risks. This includes penetration testing, design reviews, and application development/coding practices including source code reviews.

Conclusion

BlueSync technology implements strong security controls designed to enable the safe and secure use of Bluetooth Low Energy for cardiac device remote monitoring. This technology is designed to enable heart device data transfer via a patient-owned mobile platform* or a MyCareLink monitor without compromising the security of the cardiac device or patient information.

*Not presently available for use with a patient-owned mobile platform.