



## Urgent Field Safety Notice

Battery Performance Alert and Cybersecurity Firmware Updates for Certain ICD & CRT-D Devices

01 June 2018

Dear Customer,

As part of a planned series of system updates that began in 2017 with the release of Merlin@home™ v8.2.2 software, we are writing to make you aware of new firmware intended to further strengthen the security and improve the performance of our high voltage implantable cardiac devices (ICDs and CRT-Ds). The firmware upgrade is recommended for all eligible patients and includes the following updates:

1. a **battery performance alert update** to provide further detection capability for premature battery depletion in certain high voltage devices (i.e., Battery Advisory Devices), and
2. a **cybersecurity update** to provide an additional layer of protection against unauthorized device access.

This firmware upgrade will be made available following local regulatory approval. The information provided below is intended to assist clinicians and patients in understanding this firmware upgrade and the associated benefits and risks.

### **Firmware Update for Device-Based Detection of Abnormal Battery Performance in Battery Advisory Devices**

This firmware upgrade incorporates the Battery Performance Alert (BPA) for device-based detection of abnormal battery performance due to lithium cluster induced shorts in our Fortify™, Fortify Assura™, Quadra Assura™, Quadra Assura MP™, Unify™, Unify Assura™, and Unify Quadra™ devices manufactured between January 2010 and May 2015 which are subject to the October 11, 2016 Medical Device Advisory ("Battery Advisory Devices").

As communicated in August 2017, the BPA algorithm is a management tool and is intended to provide earlier notification of abnormal battery performance for Battery Advisory Devices prior to premature battery depletion. Until now, detection of this alert has only been available through the Merlin.net™ remote monitoring system and the Merlin™ programmer during routine follow-up evaluations. This firmware update now allows for device-based detection of abnormal battery performance and if BPA is triggered, a vibratory notification is delivered to the patient, thereby ensuring continuous monitoring in situations where adherence to transmission schedules is challenging (e.g., travel). Additionally, an alert will continue to be provided to physicians through the Merlin.net™ remote monitoring system and the Merlin™ programmer during follow-up evaluations.

Additional information, including the above referenced physician communications and detailed information on the BPA algorithm, testing methods and performance can be found on our website [www.sjm.com/notices](http://www.sjm.com/notices).

## **Firmware Update for Cybersecurity**

The cybersecurity firmware update provides additional security to reduce the risk of unauthorized access to the following high voltage device families that utilize wireless radio frequency (RF) communication: Fortify™, Fortify Assura™, Quadra Assura™, Quadra Assura MP™, Unify™, Unify Assura™, Unify Quadra™, Promote Quadra™ and Ellipse™.

Older generation devices (i.e., Current™ and Promote™) are not capable of accepting the firmware update due to technology limitations. If you have any concerns relating to device cybersecurity for patients implanted with Current™/Promote™ devices, you do have the option to permanently disable the RF communication capability in the device. However, if you choose that option, the patient can no longer be monitored remotely using an RF Merlin@home transmitter. For most patients, permanently disabling RF is not advisable.

As with our 2017 cybersecurity updates for pacemakers, we have received no reports of device compromise related to cybersecurity vulnerabilities in the implanted devices associated with this communication. According to the U.S. Department of Homeland Security, compromising the security of these devices would require a highly complex attack. If there were a successful attack, an unauthorized individual (i.e., a nearby attacker) could gain access and issue commands to the implanted medical device through radio frequency (RF) transmission capability, and those unauthorized commands could modify device settings (e.g., stop pacing) or impact device functionality.<sup>[1]</sup>

## **Battery Performance and Cybersecurity Firmware Upgrade Process and Associated Risks**

The firmware upgrade process takes approximately 3 minutes to complete, and during this time, the device will operate in back-up mode (VVI pacing at 67 ppm) with high voltage therapy disabled. At the completion of the upgrade, the device will return to its pre-upgrade settings. Refer to Appendix for detailed back-up mode settings including pacing outputs, and for further description of the firmware upgrade process.

As with any software update, there is the potential for a very low rate of malfunction resulting from the update. These risks do not change or increase depending on which update(s) the device is receiving (i.e., cybersecurity and/or BPA). During our recent low voltage firmware upgrade experience, there were no serious adverse events reported. Approximately 0.62% of devices experienced an incomplete upgrade and remained in the back-up pacing mode. However, in each case, the devices were restored to the prior firmware version or received the upgrade successfully after Technical Services was contacted and intervened. Additionally, a small percentage (0.14%) of patients complained of diaphragmatic or pocket stimulation or general discomfort for the time that the device was in the back-up pacing mode. **There have been no (zero) cases reported to Abbott where the device remained in back-up mode following an attempted firmware upgrade.**

Potential risks with the firmware upgrade include, but are not limited to:

- discomfort due to back-up VVI pacing settings,
- reloading of previous firmware version due to incomplete upgrade,
- inability to treat VT/VF while in back-up mode given high voltage therapy is disabled,

---

<sup>[1]</sup> Refer to the ICS-CERT Communication ICSMA-18-135-0X

- device remaining in back-up mode due to unsuccessful upgrade, and
- loss of currently programmed device settings or diagnostic data

## Patient Management Recommendations (Battery Advisory and Cybersecurity)

Prophylactic replacement of affected devices is not recommended.

### Recommendations for Devices Eligible for Firmware Upgrade

While not intended to serve as a substitute for your professional judgment, we, along with our Medical Advisory Boards, recommend the firmware upgrade for all eligible patients at the next regularly scheduled visit or when appropriate depending on the preferences of the patient and physician.

Please consider the following:

- Discuss the risks and benefits of the firmware update with your patients. As part of this discussion, it is important to consider whether the patient is implanted with a Battery Advisory device and take into account patient specific issues such as pacemaker dependence, frequency of high voltage therapy, age of device, and patient preference.
- If deemed appropriate, install this firmware update following the instructions on the programmer (and listed in the Appendix).
- The update should be performed with appropriate monitoring and external defibrillation equipment available.

The following additional recommendations **only** apply for patients implanted with Battery Advisory Devices:

- Patients receiving the firmware update should be advised that the device-based BPA will trigger a vibratory alert.
- In the absence of a BPA being triggered in a patient's device, through Merlin.net or the Merlin programmer, we continue to recommend adhering to the original patient management recommendations from the 2016 Premature Battery Depletion advisory (refer to Appendix). However, if the BPA is triggered, **immediate device explant and replacement is recommended.**

### Recommendations for Current™ & Promote™ Devices not Eligible for Cybersecurity Firmware Update

For most patients, permanently disabling RF is not advisable given the proven benefits and improved survival associated with home monitoring.<sup>[2,3]</sup> If you have any concerns relating to device cybersecurity for those patients implanted with Current™/Promote™ devices, you do have the option to permanently disable the RF communication capability in the device. However, if you choose that option, the patient can no longer be monitored remotely using an RF Merlin@home transmitter. Therefore we, along with our Medical Advisory Boards, recommend the following:

- Discuss the risks of cybersecurity vulnerabilities and proven benefits of remote monitoring with your patients at the next regularly scheduled visit.

---

<sup>2</sup> Mittal, S., Piccini, J., Fischer, A., Snell, J., Dalal, N., & Varma, N. (2014, May). *Remote monitoring of ICD patients is associated with reduced mortality irrespective of device type*. Presented at the meeting of the Heart Rhythm Society, San Francisco, CA. This was a retrospective data review and had limitations.

<sup>3</sup> Mittal, S., Piccini, J., Fischer, A., Snell, J., Dalal, N., & Varma, N. (2014, May). *Increased adherence to remote monitoring is associated with reduced mortality in both pacemaker and defibrillator patients*. Presented at the meeting of the Heart Rhythm Society, San Francisco, CA. This was a retrospective data review and has limitations.

- If deemed appropriate, RF communication may be permanently disabled during an in-clinic device interrogation with Merlin programmer software version 24.2.x or later by selecting the RF icon in the upper left corner of the FastPath summary screen.

If you have any questions about this device firmware update, you can contact your Abbott representative or our dedicated customer technical support hotline at +46-8474-4147 (EU). Additional materials, including a Patient Communication, can be found on [www.sjm.com/notices](http://www.sjm.com/notices).

Technology and security are always evolving, and Abbott is committed to ensuring our products include the latest advancements and protections for your patients. Your feedback is important to us, so please contact your Abbott representative with any questions or comments related to this update.

Sincerely,



Robert Blunt  
Divisional Vice President, Quality  
Cardiac Rhythm Management

*CC: Chairman Medical Board and relevant Head of Departments*