Abbott

# URGENT FIELD SAFETY NOTICE

## Information About Cybersecurity Update for Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ and Assurity MRI™ devices

28 August, 2017

Dear Doctor,

We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency (RF) communications (i.e., Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ and Assurity MRI™). This firmware update provides an additional layer of security against unauthorized access to these devices that further reduces the potential for a successful cybersecurity attack.

This release will be launched following local regulatory approval and is part of planned updates that began with the January 2017 enhancements of the Merlin@home™ v8.2.2 software. The update contains a software release for Merlin™ programmers (version 23.1.2) including data encryption, operating system patches, and disabling network connectivity features in addition to the firmware update.

The information provided below is intended to assist clinicians and patients in understanding the cybersecurity vulnerability, the firmware update, and associated benefits and risks.

**Description of Cybersecurity Vulnerability and Associated Risks**

We have received no reports of device compromise related to the cybersecurity vulnerabilities in the implanted devices impacted by this communication and continued implant of the current firmware until the local regulatory approval of the new firmware is appropriate for patients who need pacemaker therapy. According to the US 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. [1]

[1] Refer to the ICS-CERT Communication ICSMA-17-241-0X Abbott Laboratories Accent/Anthem Accent MRI Assurity/Allure and Assurity MRI Pacemaker Vulnerabilities

## Firmware Update Details and Associated Risks

Firmware refers to the particular kind of software that is embedded in the hardware of the pacemaker device. The firmware update process takes approximately 3 minutes to complete, and during this time, the device will operate in back-up mode (VVI pacing at 67 bpm), and essential, life-sustaining features remain available. At the completion of the update, the device will return to its pre-update settings.

Based on our previous firmware update experience, as with any software update, there is a very low rate of malfunction resulting from the update. These risks (and their associated rates) include but are not limited to:

- reloading of previous firmware version due to incomplete update (0.161%),
- loss of currently programmed device settings (0.023%),
- complete loss of device functionality (0.003%), and
- loss of diagnostic data (not reported).

## Patient Management Recommendations

Prophylactic replacement of affected devices is not recommended.

While not intended to serve as a substitute for your professional judgment as to whether the firmware update is advisable for a particular patient, we, along with our Cyber Security Medical Advisory Board, recommend the following:

1. Discuss the risks and benefits of the cybersecurity vulnerabilities and associated firmware update with your patients at the next regularly scheduled visit. As part of this discussion, it is important to consider patient specific issues such as pacemaker dependence, age of device, and patient preference and provide them with the "Patient Communication".

2. Determine if the update is appropriate given the risk of update for the patient. If deemed appropriate, install this firmware update following the instructions on the programmer (and listed below).

3. For pacing dependent patients, consider performing the cybersecurity firmware update in a facility where temporary pacing and pacemaker generator change are readily available, due to the very small estimated risk of firmware update malfunction.

## Firmware Update Process

During the firmware update process the device will be temporarily placed in a back-up mode. Clinicians are advised to record the programmed device settings before the update in case they are not properly restored after the update. The process for the update is as follows:

- **Abbott Representatives will update the Merlin™ programmer with new software**: The new programmer software will allow for device firmware to be updated.

- **The Programmer provides a prompt when a device is interrogated**: After the programmer has been updated and the device has been interrogated, the programmer will provide an alert that an update is available. Before viewing the alert, device programmed parameters may be printed out as a record of the pre-update settings.

- **A follow up on-screen prompt is displayed on programmer**: The physician will follow the on-screen instructions to continue.

- **The physician selects the cybersecurity firmware update**: The programmer will download new firmware to the patient's device. The cybersecurity firmware update cannot be delivered remotely.

- **The download to device should complete within approximately three minutes**: The telemetry wand must remain over the device until completion of the firmware update.

- **After the update, verify that the device is functioning appropriately and not in back-up mode:** Check that the device parameters have been restored to the pre-update settings after the update and confirm that diagnostic data are still present. If either of these does not occur, repeat the process and/or contact Abbott technical support.

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

Abbott will continue to make security updates across the devices within our portfolio as part of our ongoing commitment to design safe, effective and secure products for our patients. Your feedback is important to us, so please contact your Abbott representative with any questions or comments related to this update.

Sincerely,

Susan Jezior Slane
Divisional Vice President, Global Quality Systems and Compliance
Cardiovascular and Neuromodulation