

APHRS Advisory Notice 1th December 2017

Device: Information About Cybersecurity for Accent™/Anthem™/Accent MRI™/AccentST™/Allure™ and Assurity MRI™ and Assurity MRI™ devices

Description: Communication and installation guides of new pacemaker firmware (software) intended to address the risk of unauthorised access to the above mention pacemakers relating to previous Safety alert released August 28th (RC-207-RN-01124-1).

The firmware is to be released December 2017 and includes general software upgrades and will be loaded onto the Abbott (previously St Jude Medical) programmer.

Description of Cybersecurity Vulnerability and Associated Risks.

Abbott has not received any reported cases of compromised related to cybersecurity in any of their devices. US department of Homeland security have advised that unauthorised access to a device would require a highly complex attack with the culprit within near proximity of the device. If access were able to be obtained the attacker could issue commands to alter pacing function.

Firmware Upgrade Details

Firmware refers to a type of software that is embedded in the hardware of the pacemaker device. The upgrade takes approximately 3 minutes to complete and during this time the device will operate in backup VVI mode at 67 bpm. At the completion of the upgrade the device will return to the pre update parameters.

Risk: There is a very low risk of malfunction during upgrade, these include but are not limited to:

- Reloading of previous firmware version due to incomplete upgrade (0.61%)
- Loss of currently programmed device settings (0.23%)
- Complete loss of device function (0.003%)
- Loss of diagnostic data (not reported)

Additionally, some patients with VA conduction may become symptomatic with VVI pacing during the upgrade.

Presentation: On interrogation of the devices with firmware upgrade, it will be highlighted under the ALERT's option in the front screen. This will direct you to the to the firmware upgrade. It does not install automatically.

Advice:

Prophylactic replacement of devices is not recommended.

The patient should be assessed for pacemaker dependency and symptomatic VA conduction prior to deciding whether to install the upgrade. The risk of the software update must be taken into consideration and discussed with patients. If the decision is to proceed to installing the firmware upgrade the following precautions are required:

- Pacemaker dependent patients should be upgraded where temporary pacing is available. The facility needs to have the ability to perform generator changes or at least be able to promptly transfer patients to a referral centre that can perform this procedure.
- Patients with symptomatic VA conduction should have the upgrade downloaded in a supine position and be observed during the upgrade process.

Process of the upgrade

- The programmer provides a prompt when the device is interrogated, this appears under the ALERT menu. Prior to selecting this option the current device parameters should be printed out as a reference.
- Select the device alert and follow the on screens prompts.
- Select cybersecurity firmware upgrade and confirm download. The upgrade will take approximately 3 minutes
- On completion of the upgrade the initial parameters should be verified with the current parameters of the pacemaker to ensure original parameters have been reinstalled.