A Patient's Guide to the New Pacemaker Firmware Update

At Abbott, we put your health and safety at the heart of everything we do.

We want to inform you about an update to the firmware installed on your pacemaker that further strengthens protections on your device to prevent anyone other than your doctor from changing the settings on your pacemaker. This update is part of Abbott's ongoing commitment to continuously improve patient care.

Firmware is a kind of software that is embedded in the hardware of the pacemaker device. Technological devices that use software, such as that in your pacemaker, require updates from time to time. At Abbott, we're always working to improve the performance, safety, and security of our products, and to make those improvements available to all patients.

Connected devices are having a significant positive impact for patients and their health. To protect you, Abbott has developed new firmware with additional security measures that can be installed on your pacemaker. In January 2017, we released security updates for our Merlin™ remote monitoring system that is used with implantable pacemakers and defibrillators. They also included additional security measures for Merlin@home to prevent remote unauthorized access to your pacemaker. At that time, we indicated that the company would continue to implement additional updates.

To help keep you informed, this patient guide provides responses to Frequently Asked Questions (FAQ) related to the new pacemaker firmware update. In addition, if you have any further questions about the pacemaker firmware update, please contact our dedicated hotline at 1-800-722-3774 (U.S.) or visit our website at sjm.com/cyberupdate. As always, you should discuss the risks and benefits of any medical procedure with your doctor.

FAQ

1. **What is the purpose of the new pacemaker firmware update?**

   The pacemaker firmware update provides an additional layer of security for your pacemaker. This planned update is intended to prevent anyone other than your doctor from changing your device settings. Abbott is not aware of any reports of unauthorized access to any patient's implanted pacemaker. Abbott continues to

make our products more secure for customers and patients, including with this series of planned system updates.

2. What do I need to know about the new pacemaker firmware update process?

Abbott's recommendation, and that of our Cyber Security Medical Advisory Board, is that you have a conversation with your physician to determine if the update is right for you. If you and your physician decide that the pacemaker firmware update is right for you, it can be performed during your next regularly scheduled in-office visit. During the process a wand will be placed over your pacemaker during the update and final settings will be reviewed following the update to ensure that the update has been completed. The process takes approximately three minutes to complete.

3. How do I know if I need the new pacemaker firmware update?

Every patient's circumstance is unique. For this reason, we encourage you to discuss this update with your physician. In some cases, doctors and patients will decide that the risks that could be associated with performing the new pacemaker firmware update for some patients may outweigh the benefits. If you do not receive the update, your pacemaker will continue to function as intended, and you can receive the update at any future time.

The pacemaker devices to which this update applies include the RF telemetry versions of the following devices in the U.S.: Accent SR RF™, Accent MRI™, Assurity™, Assurity MRI™, Accent DR RF™, Anthem RF™, Allure RF™, Allure Quadra RF™, and Quadra Allure MP RF™

The pacemaker devices to which this update applies include the RF telemetry versions of the following devices outside of the U.S.: Accent SR RF™, Accent ST™, Accent MRI™, Accent ST MRI™, Assurity™, Assurity +™, Assurity MRI™, Accent DR RF™, Anthem RF™, Allure RF™, Allure Quadra RF™, Quadra Allure MP RF™, Quadra Allure™, and Quadra Allure MP™. We are communicating with regulators to implement the update globally.

The update will be made available to current patients. Every pacemaker manufactured beginning August 28, 2017 will have this update pre-loaded in the device.

4. What are the risks associated with the new pacemaker firmware update?

We are anticipating the update will occur as planned. However, as with any firmware update, there is a very low rate of malfunction resulting from the update. We encourage you to discuss the risks and benefits of receiving the update with your doctor.

5. **How likely is it that someone could gain unauthorized access to my device?**

   We have received no reports of unauthorized access to any patient's implanted pacemaker. According to the advisory issued by the U.S. Department of Homeland Security, compromising the security of these devices would require a highly complex set of circumstances. [1]

6. **Does this mean I should have my pacemaker removed?**

   No, preventative replacement is not necessary or recommended. Your pacemaker remains fully effective for providing pacing, as designed.

7. **Should I continue to use my home monitor?**

   Yes, you should continue to use your Merlin@home™ device as it allows your physician to more frequently receive, assess, and monitor your device's function.

---

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