Abbott Issues New Updates For Implanted Cardiac Devices

-Planned updates designed to provide new patient management tools and further protection against unauthorized access

- Updates part of ongoing effort to continuously improve patient care

ABBOTT PARK, Ill., Aug. 29, 2017 – Today, Abbott notified physicians of updates to its implantable pacemakers and defibrillators as part of its ongoing commitment to continuously improve patient care.

The new device updates include a Battery Performance Alert for our implantable cardioverter defibrillators (ICDs) that provides physicians with earlier warning of the potential for the low risk of premature battery depletion. They also include a planned update to pacemaker firmware (a kind of software) to add additional security protections designed to reduce the risk of unauthorized access to patients' pacemakers.

"Connected devices are having a significant positive impact for patients and their health," said Robert Ford, executive vice president, Medical Devices, Abbott. "To further protect our patients, Abbott has developed new firmware with additional security measures that can be installed on our pacemakers."

There have been no reports of unauthorized access to any patient's implanted device, and according to an advisory issued by the U.S. Department of Homeland Security, compromising the security of these devices would require a highly complex set of circumstances.

Abbott is communicating with regulatory authorities worldwide to implement the new updates to the implantable devices. Abbott's recommendation, and that of its Cyber Security Medical Advisory Board, is that a patient have a conversation with their physician to determine if the update is right for them. Abbott will continue to make updates and product enhancements across its devices as part of the company's ongoing commitment to provide safe, effective and secure products for patients.

"All industries need to be constantly vigilant against unauthorized access," continued Ford. "This isn't a static process, which is why we're working with others in the healthcare sector to ensure we're proactively addressing common topics to further advance the security of devices and systems."

About the Battery Performance Alert for Implantable Cardioverter Defibrillators

In October 2016, Abbott notified physicians and patients that a subset of ICD and cardiac resynchronization therapy defibrillator (CRT-D) devices manufactured between January 2010 and May 2015 could potentially experience premature battery depletion due to short circuits from lithium clusters.

The potential for premature battery depletion in the affected devices is low. The new Battery Performance Alert can be used as a tool to further assist in identifying the potential for these devices to experience premature battery depletion.

More detailed information on the Battery Performance Alert algorithm testing methods and performance can be found on our website www.sjm.com/batteryupdate.

About the New Pacemaker Firmware Update

The new pacemaker firmware update is part of Abbott's planned enhancements that began with updates announced in January 2017 to the Merlin@home™ v8.2.2 software. The new updates provide an additional layer of security against unauthorized access to these devices.

The update contains a software release that includes data encryption, operating system patches, and the ability to disable network connectively features, in addition to the firmware update.

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™.

Every pacemaker manufactured beginning Aug. 28, 2017, will have this update pre-loaded in the device and those devices will not need to be updated. Based on Abbott's consultation with the U.S. Food and Drug Administration (FDA), this update is being treated as a field action; however, the devices continue to function as intended and replacement of implanted pacemaker devices is not recommended.

For more information about the pacemaker firmware update, please contact our dedicated hotline at 1-800-722-3774 (U.S.) or visit our website at www.sjm.com/cyberupdate.

Abbott is communicating with the FDA, the U.S. Department of Homeland Security, and global regulators, and works with leading independent security experts, to strengthen protections against unauthorized access to its devices.

This update will be released outside the U.S. following local regulatory approvals. Outside of the U.S., the pacemaker devices to which this update applies include the RF telemetry versions of the following devices: 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™.

Abbott has additional resources available on its website to address questions from physicians and patients about these updates

at www.sjm.com/cyberupdate and www.sjm.com/batteryupdate.

About Abbott

At Abbott, we're committed to helping people live their best possible life through the power of health. For more than 125 years, we've brought new products and technologies to the world – in nutrition, diagnostics, medical devices, and branded generic pharmaceuticals – that create more possibilities for more people at all stages of life. Today, 94,000 of us are working to help people live not just longer, but better, in the more than 150 countries we serve.

To learn more about Abbott's commitment to protecting our devices, products and systems, please read our commitment to cybersecurity on the Abbott website.

Connect with us at www.abbott.com, on Facebook at www.facebook.com/Abbott and on Twitter @AbbottNews and @AbbottGlobal.

For further information: Abbott Media: Candace Steele Flippin, (651) 756-3029, Jonathon Hamilton, (224) 667-8646; Abbott Investor Relations: Mike Comilla, (224) 668-1872