BIOTRONIK Statement on the Medical Advisory and Safety Communication Regarding Medtronic's Conexus Radio Frequency Telemetry Protocol

March 22, 2019

Executive Summary

The Department of Homeland Security and the US FDA have issued a Medical Advisory and Safety Communication respectively describing two types of cybersecurity vulnerabilities affecting multiple Medtronic devices that utilize the Conexus telemetry protocol. BIOTRONIK utilizes substantially different protocols for both the clinical and the home environment. Moreover, by design, the remote communication system via BIOTRONIK Home Monitoring® does not have the functionality to transmit or alter therapeutic commands to the implant.

Full Statement

On March 21, 2019, the Department of Homeland Security issued a Medical Advisory describing two types of cybersecurity vulnerabilities affecting multiple Medtronic devices that utilize the Conexus telemetry protocol. Correspondingly, the US Food and Drug Administration (FDA) issued a Safety Communication, similarly describing how the Conexus wireless telemetry protocol has cybersecurity vulnerabilities. The FDA has confirmed that if these vulnerabilities were to be exploited, they could allow an unauthorized individual (such as somebody other than the patient's physician) to access and potentially manipulate an implantable device.

Both the Medical Advisory and the Safety Communication refer to vulnerabilities that affect Medtronic devices in the clinical environment and the home environment.

BIOTRONIK utilizes substantially different protocols for both, (1) the wireless communication used in a clinical environment for programming implantable devices by a physician's programmer, and (2) the Home Monitoring communication used in a home environment for remote patient monitoring.

By design, the remote communication system via BIOTRONIK Home Monitoring® does not have the functionality to alter the therapeutic behavior of the implant.

It is only possible to program the implant wirelessly once a radio frequency (RF) connection has been activated using a specific bidirectional, near-field communication protocol. Technical implementation and the laws of physics limit the range of this communication to only a few meters. To activate an RF connection, the programmer wand must be placed on the patient's chest a few centimeters above the implant. By design, commands cannot be transmitted to the implant without prior activation of the RF connection in this way.

Safety is paramount to the design and production of all BIOTRONIK devices and is at the center of everything we do. As part of its established cybersecurity processes, BIOTRONIK continuously analyzes external reports and assesses device security. BIOTRONIK takes these additional steps to ensure the safety and efficacy of all of its systems.