Statement on the Cybersecurity of BIOTRONIK Solutions Following WIRED Magazine's Article on Vulnerabilities in Pacemaker Programmer Systems

August 17, 2018

On August 9, WIRED magazine reported that researchers discovered cybersecurity vulnerabilities in the way pacemaker programmers connected to the software delivery network of a specified manufacturer. The researchers claim that "digital code signing"—the cryptographic validation of the legitimacy and integrity of software—is lacking in the manufacturer's infrastructure, allowing an attacker to potentially take control of device programmers through malicious updates that can subsequently be spread to implanted pacemakers.[1]

None of BIOTRONIK's devices, programmers or networks are affected by these cybersecurity vulnerabilities. "Digital code signing" is already in use in BIOTRONIK's systems. Along with other cybersecurity mechanisms such as encrypted data transmissions via virtual private networks, this ensures a high level of security across BIOTRONIK's infrastructure.

In its commitment to developing solutions that save lives and improve patients' quality of life, BIOTRONIK maintains a strong collaboration with the relevant authorities and regulatory bodies to uphold the highest safety and security standards.

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.

[1] Lily Hay Newman, 'A New Pacemaker Hack Puts Malware Directly on the Device', August 9, 2018, https://www.wired.com/story/pacemaker-hack-malware-black-hat/