BIOTRONIK Statement on the FDA's Safety Communication "URGENT/11"
October 4, 2019

On October 1, the US Food and Drug Administration (FDA) issued a Safety Communication regarding a set of cybersecurity vulnerabilities, referred to as "Urgent/11" that—if exploited by a remote attacker—may introduce risks for medical devices and hospital networks. According to the communication: "These vulnerabilities may allow anyone to remotely take control of the medical device and change its function, cause denial of service, or cause information leaks or logical flaws, which may prevent device function."

These vulnerabilities exist in a third-party software component known as IPnet, which supports network communications between computers. BIOTRONIK's medical devices, systems and networks do not incorporate IPnet and are therefore not affected by these vulnerabilities.

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.