Cybersecurity and Remote Medical Devices: Matters of the Heart

When it comes to maximizing efficiency in healthcare, remotely-monitored devices represent a new frontier in advancement…but they also present new challenges. Perhaps no one is more aware of that than the device manufacturers themselves.

When you think of cybersecurity, you probably think of bank accounts and credit cards. But with burgeoning technology comes new pockets of vulnerability, and therefore expanded areas requiring protection. And in healthcare, those issues quite literally involve matters of the heart.

FDA identifies cyber-risks in some cardiac devices

Early last month, the U.S. Food and Drug Administration (FDA) released a Safety Communication outlining dangers inherent in vulnerabilities in some St. Jude Medical implantable cardiac devices, as well as their corollary, the Merlin@home Transmitter. These data-transmission devices permit doctors to remotely monitor patients around the clock after discharge, thereby reducing the need for frequent office visits and simultaneously equipping physicians with vital information when it's most needed.

Although the FDA stated that the cyber-vulnerabilities in question had not brought any harm to patients (the potential scenarios include an unauthorized user accessing the devices remotely and interfering with the programming, causing the battery to drain quickly or bringing about harmful pacing or electrical charges to the heart), the agency is determined to make device manufacturers in general aware of the risks with the goal of creating new protections and implementing constant, ongoing vigilance.

Suzanne B. Schwartz, M.D., M.B.A., is FDA's Associate Director for Science and Strategic Partnerships at the Center for Devices and Radiological Health. She authored a post that appeared on the FDA's blog in December. In it, she stated: "Protecting medical devices from ever-shifting cybersecurity threats requires an all-out, lifecycle approach that begins with early product development and extends throughout the product's lifespan."

St. Jude files defamation suit after researchers release inflammatory report

Last August, cybersecurity research firm MedSec teamed up with investment researcher Muddy Waters Research and issued a report that alleged the discovery of weaknesses in St. Jude cardiac devices that could leave the door

open to cyber-attacks. Although there was no corroboration for the next claim, the report said that the devices would probably soon be yanked from the market. It also suggested that current users should unplug their devices at home so as to end the remote monitoring.

The FDA rejected the researchers' monitoring-interruption advice and said that the devices offered health benefits for patients substantial enough that any potential risks were negligible in comparison. This seemed to only inflame Muddy Waters, which subsequently released a video of what it claimed was a cyber-attack on the St. Jude Medical pacemaker. (University of Michigan researchers cautioned that they saw the video as lacking validity.)

St. Jude filed a defamation suit against Muddy Waters and MedSec, alleging that the former pursued unjust enrichment "by publicly disseminating false and unsubstantiated information" that deceived and alarmed patients. The device manufacturer argued that "defendants must be held accountable so that such activity will not be incentivized and repeated in the future."

Further, St. Jude put checks in place to let patients know that it prioritized cybersecurity, including the forming of a Cybersecurity Medical Advisory Board in October. And when the FDA located potential weak spots in the area of device cybersecurity, St. Jude came back (on that very day) with a software solution that the agency approved.

Cybersecurity: vigilance that's here to stay

In her blog post, the FDA's Schwartz highlighted the need for medical device manufacturers to begin with a thoughtful product: "Manufacturers should build in cybersecurity controls when they design and develop the device to assure proper device performance in the face of cyber threats," but not to stop there. She urged them to make a habit of continually monitoring potential threats so as to stay ahead of hackers, rather than viewing the strengthening of security measures as a discrete effort.

"Today's postmarket guidance recognizes today's reality," she wrote. "Cybersecurity threats are real, ever-present, and continuously changing. In fact, hospital networks experience constant attempts of intrusion and attack, which can pose a threat to patient safety. And as hackers become more sophisticated, these cybersecurity risks will evolve."

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.