AdvaMed, the Advanced Medical Technology Association
Statement for the Record

Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade and Subcommittee on Communications and Technology
"Understanding the Role of Connected Devices in Recent Cyber Attacks"

Wednesday, November 16, 2016

AdvaMed is the world's largest trade association representing medical technology manufacturers. AdvaMed member companies produce the medical devices, diagnostic products and health information systems that are transforming health care through earlier disease detection, less invasive procedures and more effective treatments.

Patient safety is critical to the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where the risks, no matter how remote, evolve.

Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment and maintenance of the device. Similarly, manufacturers implement proactive and risk-based approaches to manage medical device cybersecurity, including the use of "good cyber hygiene" through routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

It is important that whenever potential vulnerabilities involving a medical device are discovered, such findings should first be brought to the attention of the manufacturer for review, analysis, and possible remediation. Any other approach potentially places patients' lives at risk.

Additionally, medical technology cybersecurity is a shared responsibility among all stakeholders, including manufacturers, hospitals, physicians, and users. Device manufacturers play an important role; however, all stakeholders within the larger system must work together to ensure system-level integrity.

The medical technology industry is actively working with FDA and other key stakeholders to raise awareness about potential cybersecurity concerns, and we look forward to working with all stakeholders to further these efforts.