STRATEGIC MANAGEMENT SERVICES

OIG Testimony on FDA Oversight of Cybersecurity Risks to Medical Devices

By Richard Kusserow | April 2, 2020

Reminder to Compliance Officers that medical devices can be a cybersecurity risk

The Department of Health and Human Services (HHS) Office of Inspector General (OIG) provided Congressional testimony regarding identified safety and effectiveness concerns associated with the Food and Drug Administration's (FDA) oversight of medical devices. The testimony stated that the FDA needs to take steps to mitigate the risk of cybersecurity threats to medical devices. As more medical devices use wireless, internet, and network connectivity to store and transport sensitive data, the safety of these devices is an area of increasing concern for the OIG. The OIG noted that researchers have shown that FDA-approved networked medical devices can be susceptible to cybersecurity threats, such as ransomware and unauthorized remote access, if the devices lack adequate security controls. These networked devices include pacemakers, hospital-room infusion pumps, and diagnostic imaging devices. The OIG cited two of its reports, one from September 2018 and the other from October 2018, assessing the FDA's oversight of pre-market and post-market cybersecurity risks to medical devices. Both reports called for the FDA to take further action in addressing cybersecurity threats to medical devices in an effort to reduce risk to patients and the health care industry. In the October 2018 report, the OIG recommended that the FDA: (1) continually assess the cybersecurity risks to medical devices and update, as appropriate, its plans and strategies; (2) establish written procedures and practices for securely sharing sensitive information about cybersecurity events with key stakeholders who have a "need to know"; (3) enter into a formal agreement with Federal agency partners, namely the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, establishing roles and responsibilities as well as the support those agencies will provide to further the FDA's mission related to medical device cybersecurity; and (4) ensure the establishment and maintenance of procedures for handling recalls of medical devices vulnerable to cybersecurity threats. The FDA agreed with the recommendations and moved to act upon them by making administrative changes to its pre-market and post-market processes. It released draft guidance encouraging device manufacturers to meet with the FDA early on and discuss how they are addressing cybersecurity in their device's design and development. They also made post-market improvements to the procedures for handling recalls of medical devices vulnerable to cybersecurity threats, including the signing of a Memorandum of Agreement with the Department of Homeland Security, to improve information sharing of cybersecurity vulnerabilities and coordinate response actions. All of this is a reminder for Compliance Officers to ensure that their organization's HIPAA Security practices are addressing medical devices vulnerabilities.