COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 11. November 30, 2018 OIG Audit Asserts Concerns About FDA Oversight of Device Security

By HCCA Staff

The security of medical devices has long been a worry for covered entities and some business associates, with fears intensifying as more are connected to the internet. Often the main challenge has been the reluctance, if not downright refusal, of manufacturers to provide patches and updates to address vulnerabilities, claiming they were forbidden to do so by the Food and Drug Administration (FDA).

In 2013, while warning that devices were vulnerable to cyberattacks, FDA actually had to issue a statement correcting the misperception that it didn't allow patches (*RPP 7/13, p. 1*). In 2014, agency officials pledged to begin looking at device security through the "total product lifecycle" (*RPP 10/14, p. 4*). The agency has issued a host of draft and final guidance documents since that time, and has "taken significant steps…towards the vision of a healthy and resilient cyber ecosystem."

But a recent audit by the HHS Office of Inspector General (OIG) found that FDA is falling short on device security. The audit, released Nov. 1, is titled "The Food and Drug Administration's Policies and Procedures Should Better Address Postmarket Cybersecurity Risk to Medical Devices."

Oversight Follows Assessments

As OIG explained, FDA's lifecycle approach to security consists of pre- and postmarket approvals and requirements. Security falls under FDA's Center for Devices and Radiological Health (CDRH).

"In the premarket phase, FDA assesses whether a medical device is safe and effective for its intended use. To receive FDA clearance or approval to market a medical device in the United States, a manufacturer must submit to FDA proper documentation showing that its device is safe and effective. In the postmarket phase—after FDA clears or approves a medical device—FDA conducts oversight activities, such as monitoring and investigating the medical device's safety and effectiveness, and alerting the public of problems when warranted," OIG said. "Postmarket requirements for medical device manufacturers include the tracking and reporting of device malfunctions, serious injuries, and deaths; reporting corrections and removals; registering establishments; and compliance with quality system regulation."

To complete its audit, OIG "reviewed FDA's policies, procedures, manuals, and guides; interviewed staff; and reviewed public information available on FDA's website. We also analyzed FDA's processes for receiving and evaluating information on medical device compromises. In addition, we tested CDRH's internal controls to determine whether they ensured an effective response to a medical device cybersecurity incident," the audit said. Field work was undertaken from September 2016 to February 2017.

During the audit, OIG "did not identify evidence that FDA mismanaged or responded untimely to a reported medical device cybersecurity event." But the oversight agency determined that "FDA had not sufficiently assessed the risks of medical device cybersecurity events." As a result, FDA's "existing policies and procedures did not include effective practices for responding to those events," OIG said.

Broadly speaking, "FDA's efforts to address medical device cybersecurity vulnerabilities were susceptible to

inefficiencies, unintentional delays, and potentially insufficient analysis," OIG concluded. It also issued a series of recommendations, some of which FDA accepted.