OIG Audit Finds Weak Spots in FDA's Medical Device Cybersecurity Protocol

One of the many tasks assigned to the U.S. Food and Drug Administration (FDA) is ensuring that every medical device that makes it to market includes cybersecurity sufficient to prevent a cyberattack that might interfere with the device's functioning. The Health and Human Services' Office of Inspector General (OIG) recently released the results of an audit of the FDA's protocol for assessing cybersecurity in postmarket medical devices. Unfortunately, the FDA didn't emerge from the audit without the proverbial reprimand.

Two FDA district offices missing written SOPs

Regarding the workflow for managing cybersecurity events (such as breaches or attacks), the OIG determined that the FDA's policies and procedures are not consistently sufficient for the important and sensitive task at hand. A total of 19 FDA offices underwent review for the OIG report. When it came to medical devices that have certain weak spots that hackers might use to collect patient data or use to maliciously enter healthcare networks, the OIG auditors discovered that standard operating procedures for how to handle the recall of devices were not in writing and had not been established in two of the FDA district offices under audit.

The OIG acknowledged that the FDA has created procedures for how to handle cybersecurity events, but said that whether or not the agency could adequately deal with the issues was still up in the air; the OIG felt FDA response to events had not been thoroughly tested thus far. And furthermore, the OIG determined that the FDA's attempts to shore up weak cyber spots in medical devices were plagued by "inefficiencies, unintentional delays, and potentially insufficient analysis."

With that said, though, the OIG also noted that even in the presence of those aforementioned inefficiencies, the FDA isn't necessarily guilty of mismanagement, stating: "We did not identify evidence that FDA mismanaged or responded untimely to a reported medical device cybersecurity event."

What to do about it?

Some of the recommendations from the OIG to the FDA include:

- Collaborate with the Department of Homeland Security's Industrial Control Systems Cyber-Emergency Response Team in order to set up specific responsibilities and designate individuals for carrying out those responsibilities
- Develop protocols, and memorialize them in writing, for how to handle sensitive information when sharing news of cybersecurity events with stakeholders who need to be informed of them
- Regarding the recall of medical devices that are at risk of cybersecurity attacks, establish policies and procedures to follow during those events
- Continue to address the issue of medical device cybersecurity and update plans as specific threats change

The OIG's report acknowledges that the FDA had already addressed some problem spots after the audit took place and before the report was released. And for the FDA's part, although the agency said the report presented an "incomplete and inaccurate" snapshot of its medical device cybersecurity, it did not dispute any of the OIG's recommendations.

However, the agency did push back at the OIG's conclusion that the FDA was operating under inadequate policies or procedures in this area. Similarly, the FDA disagreed with the OIG's finding that the FDA had not sufficiently addressed device cybersecurity at the component level.

advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

NELSON HARDIMAN
HEALTHCARE LAWYERS