FDA Urged to Boost Cybersecurity Scrutiny for Premarket Medical Devices

Huge swaths of daily life depends on access to the internet. Healthcare is no exception. But of course increased dependence comes with increased vulnerability. And the government is taking note when it comes to a very specific area of healthcare.

Earlier this month, the Health and Human Services Office of the Inspector General (HHS-OIG) released a report that speaks to the intersection of the U.S. Food and Drug Administration (FDA) and the issue of cybersecurity in medical devices . . . before those devices even make it to market.

FDA advised to add cybersecurity queries to early stages of submission review

The OIG's report suggested that the FDA broach cybersecurity questions and concerns with medical device manufacturers at the presubmission stage of meetings. Further, the FDA was urged to update its review guide for medical device submissions (known as the Smart template) with cybersecurity questions.

Additionally, the OIG advised the FDA to revise its Refuse-to-Accept checklist (RTA) by adding a requirement for cybersecurity documentation.

The RTA checklist gives the FDA the means for rejecting a medical device submission before the thorough review stage. If a manufacturer has not satisfied all items on the list, the FDA has the right to put the application on hold until the missing piece is supplied. Adding proof of cybersecurity to the RTA document would be a novel step for the FDA, one with which the FDA agrees:

"We believe that including cybersecurity as an item on the list could improve review efficiency by ensuring that the file containing all the necessary elements before the review is initiated rather than asking for such information, if not already in the premarket submission, during the review."

OIG conducted its own reviews and interviews

The OIG's report didn't originate from mere common sense suggestions, however. Rather, it was built upon interviews of FDA staff by the OIG, the examination of nearly two dozen medical device submissions (including notes by FDA reviewers pertaining to devices approved in 2016), and the review of FDA guidance documents, policies, and procedures for both cybersecurity and the medical device review process overall.

"As the Federal agency responsible for regulating these devices, FDA may consider the cybersecurity risks and controls in its overall assessment of a device's safety and effectiveness. Ultimately, FDA determines whether a networked medical device may be legally marketed in the United States," the report stated.

The OIG did not overlook measures the FDA has already taken when it comes to cybersecurity risks in medical devices. Those initiatives include guidance documents addressing cybersecurity in medical devices, outreach events designed to inform and educate stakeholders, the development of an FDA cybersecurity work group, and the review of cybersecurity data in networked medical device submissions.

Medical device submission reviewers at the FDA let the OIG know that they do look through the lens of existing

cybersecurity vulnerabilities and risks when they are considering networked devices.

From the report: “For example, if FDA identifies a cybersecurity threat to a certain cardiac device from a specific manufacturer, it considers that same threat in evaluating submissions for similar cardiac devices from other manufacturers.”

FDA reviewers are free to ask manufacturers to supply more information during the submission process when cybersecurity documentation is on the thin side. The submission data that reviewers are typically on the lookout for may involve hazard analyses outlining device cyber-vulnerabilities, as well as steps for strengthening those potentially weak spots.

OIG believes FDA can advance further on the cybersecurity front

But the OIG sees room for improvement in the FDA’s current approach. Says the report: “However, FDA could do more to integrate its assessment of cybersecurity for networked medical devices into its premarket review process. From our observations, FDA is making limited use of key tools that could support consistency, efficiency, and effectiveness in its premarket review of cybersecurity.”

The FDA pointed out that it presently makes use of presubmission meetings with medical device manufacturers to address cybersecurity concerns. However, the agency agreed to “specifically mention cybersecurity in the next planned update of our presubmission guidance to further promote the use of presubmissions for cybersecurity questions.”