# PUBLICATION

## FDA to Provide Further Guidance for Review of Cybersecurity in Premarket Review for Medical Devices

**September 19, 2018**

**The FDA will be responding to the recent report from OIG issued this month regarding the FDA's review of medical devices that pose cybersecurity risks. Cybersecurity risks arise when networked medical devices cleared through the 510(k) process or approved through the PMA process by FDA can be susceptible to cybersecurity threats. Such cybersecurity threats include ransomware and unauthorized remote access, if the devices lack adequate security controls. To the extent medical devices are connected via wireless, Internet and other networked means, there is a risk they might not operate as intended. This could include an unauthorized access; unauthorized modification; misuse or denial of use; or unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient. Such threats can be life-threatening for patients that rely on these devices such as hospital infusion pumps, diagnostic imaging equipment and pacemakers as examples.**

Presently, the FDA has been following its Guidance document, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, issued October 2, 2014 and 21 CFR 820.30 Subpart C Design Controls for Quality System Regulations for reviewing submissions of medical devices which are vulnerable for cyber-attacks. While this has provided guidance for review of these devices, the FDA itself sees the medical device cybersecurity threat as one that is always evolving. The FDA has modified its review of manufacturer's submissions over time for establishing design controls to mitigate these risks, and hazard analysis. Such modifications are made as the Agency becomes aware of new risks from manufacturers and applies that knowledge to pending like submissions.

OIG deemed it important to evaluate the present FDA review process of cybersecurity premarket review of medical device submissions since there have been so many medical technology advancements which include a new generation of functionalities such as wireless, Internet and network connectivity. The review entailed interviewing both FDA staff who carry out and manage the review and members of the FDA's Cybersecurity Workgroup. The OIG reviewed a nonrepresentative sample of 22 submissions and FDA review notes and FDA present policies, procedures and guidance documents related to its medical device review process and to cybersecurity. *(See "FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices.")*

OIG observed that FDA often requires supplemental cybersecurity information from manufacturers where it determines the information provided in a submission is not adequate for hazard analysis related to its use of software or network connectivity. However, OIG concluded that the Agency has not been consistent in the information required for these types of submission.

The report indicates FDA has not fully integrated cybersecurity into two types of written tools that FDA reviewers use to facilitate their reviews of networked medical devices; (1) the FDA's Refuse-to-Accept Checklist (which it uses to screen 510(k) and PMA submissions for completeness) does not include a check for cybersecurity information and (2) the FDA's Smart Template for review of submissions does not prompt FDA reviewers to specifically consider cybersecurity questions.

The FDA has responded to the OIG report and concurred with the OIG's conclusions. FDA has already started to take steps to implement these suggestions. FDA has emphasized that addressing cybersecurity for networked medical devices is a responsibility shared among stakeholders, including the Agency, device manufacturers and health care providers.

Going forward, both the OIG and FDA agree the following will be included in the 510(k) and PMA review process for medical devices with potential cybersecurity threats: (1) Promote the use of presubmission meetings to address cybersecurity-related questions; (2) Include cybersecurity documentation as a criterion in FDA's Refuse-to-Accept Checklist; and (3) Include cybersecurity as an element in the Smart Template.

For more information on documentation required for a medical device submission with potential cybersecurity risks which may also include mobile devices, considered as medical devices, contact any member of Baker Donelson's FDA Group.