Buchalter
CLIENT ALERT

April 17, 2023

From Heart Monitors to Hack Monitors: Medical Device Cybersecurity

By: Meghna Parikh

ALERT: Recent guidance from the Food and Drug Administration ("FDA") clarifies a procedural issue for premarket submissions related to cybersecurity of medical devices and emphasizes the importance of collaboration between the FDA and medical device manufacturers. Providers using medical devices in their practice should pay attention to these rulings because they impacts the providers' ability to educate and engage their patients.

SUMMARY: As the healthcare industry becomes increasingly reliant on technology, medical device cybersecurity has become a critical concern not just for manufacturers, but also for providers and patients. New legislation addressing cybersecurity requirements for medical devices and recent guidance from the FDA highlight the importance of addressing cybersecurity risks in medical devices, as well as taking proactive steps to protect patient privacy. This is the right time to update your cybersecurity risk management program, be proactively compliant with the latest requirements and train your employees and distributors on the importance of cybersecurity.

Existing Legislation and Guidance

In December 2022, the Consolidated Appropriations Act of 2023 was signed into law, amending the Federal Food, Drug, and Cosmetic Act (the "Act") to include new requirements for ensuring the cybersecurity of medical devices. Under this legislation, the FDA has been granted increased authority to establish and enforce cybersecurity standards for medical devices, enhancing its ability to protect patient safety and hold manufacturers accountable for compliance.

To support these efforts, the FDA has released several guidance documents outlining best practices for medical device cybersecurity. The "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" guidance provides recommendations for the development, implementation, and maintenance of a robust cybersecurity quality system for medical devices, including risk management, design controls, and software validation. In the past, the FDA has also released guidance on best practices for communicating cybersecurity vulnerabilities to patients, related to radiologic devices. This guidance emphasizes the importance of timely and transparent communication with patients, clear and concise language to explain risks, and providing resources and support to address cybersecurity concerns.

Most Recent Guidance
The new requirements are being implemented without prior public comment due to the statutory timeframe for the effective date of section 524B of the Act and became effective as of March 29, 2023. The most recent guidance addresses a procedural issue regarding how the FDA will handle premarket submissions for cyber devices based on new amendments to the FD&C Act. The guidance states that the FDA generally intends not to reject premarket submissions submitted for cyber devices based solely on information required by the new amendments **before October 1, 2023**. Instead, the FDA will work collaboratively with sponsors of such premarket submissions as part of the interactive and/or deficiency review process. The FDA expects that sponsors will have had sufficient time to prepare premarket submissions that contain the required information by October 1, 2023, and may reject premarket submissions that do not meet the cybersecurity requirements after this date.

What does this mean for medical device manufacturers?
It is now a requirement that device manufacturers build cyber devices to be secure by design, and generate the requisite documentation proving compliance in their FDA regulatory submission, but also develop strategies to monitor and maintain the security of that device post-market and for the life of the device. The FDA may conduct more frequent inspections of medical device manufacturers than they did previously to assess compliance with cybersecurity standards, and also issue warning letters or initiate recalls for devices that do not meet these standards. This could lead to significant financial and reputational costs for manufacturers, as well as potential legal liability if patients are harmed as a result of cybersecurity breaches or vulnerabilities in their devices.

The potential for increased regulatory scrutiny and enforcement actions highlights the need for medical device manufacturers to prioritize cybersecurity and invest in measures to ensure the safety and security of their devices. Medical device manufacturers can reduce the risk of regulatory enforcement actions, protect patient safety, and enhance their overall reputation and success in the market by proactively updating their cybersecurity risk management program.

Non-compliance with any FDA requirement related to medical device cybersecurity is a civil offense under the Act. Violators may be subject to penalties of up to $15,000 for each violation, and up to $1,000,000 for all violations adjudicated in a single proceeding. In addition, medical device manufacturers who do not comply with these requirements may also be considered in violation of medical device application regulations.

What does this mean for providers using medical devices?
This guidance is not only relevant for those manufacturers who plan to make premarket submissions or file amendments. Healthcare providers have a duty to ensure their patients' well-being and safety. Physicians should provide information to patients about their medical condition, treatment options, and the associated risks. This includes informing patients about potential cybersecurity risks and ways to manage them.

Providers should ensure that medical device manufacturers have provided a clear and concise summary of the potential risks associated with the device, as well as instructions for patients on how to take appropriate action in response to the vulnerability. Any cybersecurity disclosures should have an

appropriate level of detail included for the intended audience. Plain language and non-technical jargon should be used when communicating cybersecurity vulnerabilities to patients. These disclosures should be updated as new information becomes available. This includes notifying patients and other stakeholders of any updates or changes to the cybersecurity vulnerability, as well as providing recommendations for mitigating potential risks.

Timely and transparent disclosure of cybersecurity vulnerabilities is essential to ensure patient privacy and maintain public trust in medical devices. Providers should remember they are often the face of these devices for the patient, and the creator of the relationship with the device – the manufacturers may not have the same opportunity to engage or educate a patient regarding their device.

Conclusion

These recent developments highlight not only the need to prioritize cybersecurity in the development and maintenance of cyber devices, but also in the training of the device manufacturer's sales and marketing teams, to allow them to effectively communicate the cybersecurity requirements that providers or users may need to wrestle with. By prioritizing cybersecurity, medical device manufacturers can enhance patient security, protect against cybersecurity threats, and ensure compliance with evolving regulatory standards. For providers, it highlights their role to ensure that patients are informed and educated about potential cybersecurity risks associated with the use of medical devices.

If you have any questions, please contact the author or your Buchalter relationship attorney.

Meghna Parikh
Attorney
(213) 891-5264
mparikh@buchalter.com