PAUL HASTINGS

Stay Current

November 2020

Follow @Paul_Hastings

Watching the Backdoor: Planning for and Responding to a Cybersecurity Incident at Medical Device Companies – An FDA Perspective

By Peter V. Lindsay, Brady K. Mickelsen, Nathan Sheers & Aaron Charfoos

Much has been written this year related to how the ongoing COVID-19 pandemic has impacted medical device companies, including business disruptions, product shortages, and other challenges. Cybersecurity, though less discussed, is another key risk that can present similar challenges for medical device manufacturers. Companies must focus both on the risk to their medical device products, as well as on the risk to enterprise systems that support the development, manufacture, and distribution of these products.

The U.S. Food and Drug Administration ("FDA") has published multiple guidance documents that provide direction on assessing and mitigating cybersecurity risk in medical devices in both the pre-market[1] and postmarket[2] context. The total product lifecycle considerations begin in the pre-market context with a comprehensive understanding of the cybersecurity risks associated with a device and the mechanisms that have been implemented to address those risks. Companies should allocate adequate resources to developing appropriate cybersecurity protections for their investigational device prior to the submission of any market authorization application to the Agency. FDA's expectations in this area continue to evolve quickly, which often necessitates close coordination with the device review team in determining what must be included in a regulatory submission to demonstrate that cybersecurity risks have been adequately addressed. Coordination with the Agency on these points frequently occurs as part of the Center for Devices and Radiological Health's ("CDRH") pre-submission process.

Over the last several years, FDA has issued a number of cybersecurity safety communications in the postmarket context that detail identified vulnerabilities that might affect a variety of different devices. Medical device companies need to actively address cybersecurity vulnerabilities and plan to be in the best position to quickly mitigate such vulnerabilities. For example, established risk management processes need to account for how the company will objectively assess device cybersecurity risk. The processes should assess the risk of patient harm by considering the exploitability of a cybersecurity vulnerability. Importantly, these risk assessments must consider not only the potential for direct harm to patients, but also the possibility of indirect harm due to any delay in care caused by a cybersecurity disruption to device operability. Estimating the probability of such an exploit can be difficult, and manufacturers can prepare by becoming proficient in cybersecurity vulnerability assessment tools or similar scoring systems. Frequently, this may require risk assessment teams to incorporate appropriate subject matter experts to help guide these assessments.

Manufacturers must also consider cybersecurity risks to their enterprise systems. Vulnerabilities in these systems may not immediately impact the medical device product, but may lead to significant business disruptions and regulatory concerns. For example, vulnerabilities may impact manufacturing and distribution systems, which may lead to supply disruptions as companies contain the potential impact and assess the causes and mitigations. Earlier this year, the Cyber Security and Infrastructure Security Agency ("CISA") warned that cyber actors continue to exploit Internet-accessible operational technology assets by obtaining initial access through the IT network before pivoting to the operational technology network.[3] If such vulnerabilities lead to disruptions in customer communications (e.g., email), companies must also consider the impact to other processes important to comply with regulatory requirements, such as laboratory information management systems, complaint handling, device repairs and servicing, and post-market vigilance. These concerns are even more prominent in an environment like the current pandemic, where remote working and electronic communications are the norm.

Cybersecurity planning sometimes receives less emphasis, as the apparent risk is not fully appreciated amidst other priorities (i.e., think of pandemic preparedness planning two years ago). The risk, however, is real—in late October, the U.S. government issued a cybersecurity advisory that described credible information of an increased threat to the U.S. healthcare sector by cybercriminals using malware and ransomware to not only hold data for ransom, but surreptitiously steal data at the same time.[4] Of course, device manufacturers are ideal targets for organizations seeking to disrupt key businesses (particularly those critical to supporting efforts to combat COVID-19) or to obtain intellectual property.

In light of these risks, medical device companies should consider reviewing—and updating—their cybersecurity risk management plans and incident response processes including, for example:

- Maintaining strong software lifecycle processes for medical devices that monitor any third-party software components for new vulnerabilities and patching regularly;
- Adapting, as necessary, medical device risk assessment processes and tools to account for cybersecurity vulnerabilities and their impact on device safety and essential performance—these processes should include participation by individuals with appropriate software expertise;
- Ensuring incident response plans include addressing both potential vulnerabilities to the medical device, as well as the enterprise systems that support device manufacturing, distribution, and servicing, and participating in tabletop exercises to ensure that those plans work in realty; and
- Considering participation in an Information Sharing Analysis Organization ("ISAO") and other third-party efforts to identify and mitigate vulnerabilities and threats.

With digital health and connected devices continuing to be in the spotlight, cybersecurity risks will persist, and likely increase, long after the COVID-19 pandemic eventually subsides. It is important that medical device companies carefully plan for these risks to avoid what can be crippling consequences for individual companies, their customers, and potentially patients.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Peter V. Lindsay
1.202.551.1922
peterlindsay@paulhastings.com

Nathan Sheers
1.202.551.1936
nathansheers@paulhastings.com

Brady K. Mickelsen
1.202.551.1954
bradymickelsen@paulhastings.com

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

[1] E.g., Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2018).

[2] E.g., Final Guidance: Postmarket Management of Cybersecurity in Medical Devices (Dec. 2016). Note that FDA has indicated that it does not intend to enforce reporting requirements under 21 CFR part 806 (corrections and removals) for cybersecurity vulnerabilities under certain circumstances, but the manufacturer must actively participate as a member of an Information Sharing Analysis Organizations ("ISAO").

[3] NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems (July 2020).

[4] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector (updated Oct. 29, 2020).