PREMIER TRANSFORMING HEALTHCARE TOGETHER®

May 10, 2024

Robert M. Califf, M.D.
Commissioner
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Submitted electronically to: http://www.regulations.gov

RE: Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act

Dear Dr. Califf:

Premier Inc. appreciates the opportunity to submit comments to the Food and Drug Administration (FDA) regarding its draft guidance to improve the cybersecurity of medical devices. Premier has frequently highlighted the need for a comprehensive regulatory framework for medical device cybersecurity, and the introduction of specific policies for internet-connected and software-based medical devices is a critical step towards reducing the cybersecurity risks of the evolving digital health environment. In our comments, Premier specifically recommends that FDA consider the following in finalizing this guidance:

- Affirming and ensuring that approval of a new device does not relieve the manufacturer of maintaining the cybersecurity of the predicate device(s);
- Prohibiting medical device manufacturers from receiving approvals for new devices when the manufacturer demonstrates an inability to reasonably maintain cybersecurity levels over an objectively-defined lifecycle;
- Leveraging real-world evidence (RWE) to define a data-driven usable lifecycle to determine how long manufacturers should be required to maintain adequate cybersecurity for the device;
- Creating an equitable mechanism for fining HDOs and device manufacturers when a cybersecurity breach does occur based upon the root cause analysis of the incident and commensurate with the findings; and
- Continuing to both evaluate the cybersecurity of new software- and algorithm-based medical devices and provide regulatory guidelines flexible enough to apply to the iterative and evolving nature of the software.

Our recommendations are described in greater detail below.

I. BACKGROUND ON PREMIER INC.

Premier is a leading healthcare improvement company and national supply chain leader, uniting an alliance of 4,350 hospitals and approximately 300,000 continuum of care providers to transform healthcare. With integrated data and analytics, collaboratives, supply chain solutions, consulting and other services, Premier enables better care and outcomes at a lower cost. Premier's sophisticated technology systems contain robust data gleaned from nearly half of U.S. hospital discharges, 812 million hospital outpatient and clinic encounters and 131 million physician office visits. Premier is a data-driven organization with a 360-degree view of the supply chain, working with more than 1,400 manufacturers to source the highest quality and most cost-effective products and services. Premier's work is closely aligned with healthcare providers, who drive the product and service contracting decisions using a data driven approach to remove biases in product sourcing and contracting and assure access to the highest quality products. In addition, Premier operates the nation's largest population health collaborative, having worked with more than 200 accountable care organizations (ACOs).

13034 Ballantyne Corporate Place
Charlotte, NC 28277
T 704.357.0022
F 704.357.6611

444 North Capitol Street, N.W.
Suite 625, Washington, DC 20001
T 202.393.0860
F 202.393.6499

PREMIERINC.COM

A Malcolm Baldrige National Quality Award recipient, Premier plays a critical role in the rapidly evolving healthcare industry, collaborating with healthcare providers, manufacturers, distributors, government and other entities to co-develop long-term innovations that reinvent and improve the way care is delivered to patients nationwide. Headquartered in Charlotte, North Carolina, Premier is passionate about transforming American healthcare.

II. REGULATORY CHANGES AND ENFORCEMENT CONCERNS IN MEDICAL DEVICE CYBERSECURITY

Premier and our member hospitals, health systems and continuum of care providers are on the front lines of mitigating cybersecurity threats and advancing patient safety, allowing the healthcare and public health sector to continue to operate its critical life-saving functions.

One area of particular concern is the cybersecurity of medical devices. Medical devices that contain software and connect to networks or other devices carry the risk of vulnerabilities to cyberattacks, and any vulnerabilities originating in device design and software management can impact healthcare facility operations, patient safety and data confidentiality and integrity. The FDA has an established role in regulating medical devices and issuing guidance to reduce cybersecurity risks for connected medical devices that share patient or other information. Last year FDA issued a guidance document, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, which applies to applications submitted to the FDA going forward. However, significant opportunities exist to ensure cybersecurity remains a top priority for medical devices that are already in use through the end of their clinically useful lifecycle.

Section 3305 of the Consolidated Appropriation Act of 2023, "Ensuring Cybersecurity of Medical Devices," amended the Federal Food, Drug, and Cosmetic Act by adding section 524B, which authorizes the FDA to require medical device manufacturers to monitor and disclose any new cybersecurity threats that may arise related to their devices, making them responsible for notifying HDOs of the presence of the risk and any recommended actions and mitigation strategies, where available.

Section 3305 also focuses on the importance and need for manufacturers to make available security patches and updates or upgrades consistently, and in a timely manner. There is particular attention around the requirement for a Software Bill of Materials (sBOM) to be provided for each device. While the aims of the statutory change and implementing guidance from FDA are laudable, operationalizing the requirements reveals significant gaps. For example, there are instances in which major security patches become necessary for the third-party operating systems upon which the medical devices are dependent. Under current law, device manufacturers may introduce variable delays while they validate the clinical performance and accuracy of their proprietary software and firmware, but they are not required to extend liability protections to HDOs during the period that the operating system remains unpatched and vulnerable.

Similar concerns arise around sBOMs, where certain disclosures are required, yet loopholes allow manufacturers to continue to skirt liability. Unfortunately, there are no codified requirements around disclosures that must be present in the sBOM that can be objectively mapped to common HDO network architecture elements and industry best practices. As a result, it is neither practical nor fully possible for an HDO to hold a device manufacturer accountable to an economically reasonable and sustainable understanding of "cybersecure." ***Premier is concerned that the current policy dynamic continues to incent manufacturers towards a strategy of creating and selling newer replacement devices - not fixing issues with existing devices.***

The need to hold manufacturers accountable for maintaining the cybersecurity of existing devices is even more critical as healthcare providers across the continuum grapple with financial strains that preclude them from continuously investing in newer technologies with limited benefit to patient care. Therefore, it is imperative that providers have confidence that a device they purchase will be serviced for its entire lifespan.

III. NEW FOCUS ON CYBER DEVICES

The additional proposed requirements for the approval and ongoing cybersecurity of cyber medical devices in this update to the FDA's Premarket Cybersecurity Guidance is an important step towards scaling up the FDA approval process for the future of digital healthcare. According to FDA data, the number of AI/ML-enabled medical devices approved alone has seen a marked increase in the past several years, exempting a brief Covid-related pause, and should see over 30 percent growth in 2024.

With this evolution in the types of medical devices seeking, and receiving, FDA approvals, the FDA must both evaluate the cybersecurity of new software-based medical devices and provide regulatory guidelines flexible enough to apply to the iterative and evolving nature of the software. While the FDA's previous Premarket Cybersecurity Guidance addresses the first of these concerns, the recent draft guidance on cyber medical devices is crucial to addressing the second. Premier specifically supports this draft guidance's alignment with Premier's recommendations around the safe, responsible, and transparent use of cyber medical devices, defined here to include internet-connected and software-based devices, that may have an evolving cybersecurity profile based on algorithmic updates.

IV. CYBERSECURITY FOR HOSPITALS

Premier strongly believes that the incentives for better medical device cybersecurity must be aligned between hospitals and medical device developers. As Premier continues to note, there is misalignment between the economic useful life of clinical equipment and the supported useful life of the same equipment. Ideally, HDOs would replace legacy medical devices when they reach a medical device manufacturer's declared end of support. However, these devices can frequently provide useful, substantially similar clinical functionality to newer models, even if the device can no longer be reasonably secured against cyber threats. Further, when HDOs do decide to replace legacy devices, these devices are occasionally sold on the secondary market to less-resourced HDOs which are even less capable of managing the growing cybersecurity risk to these devices over time.

Should medical device manufacturers seek approval for new devices via a 510(k) process, ***Premier believes that approval of a new device should not relieve the manufacturer of maintaining the cybersecurity of the predicate device(s)*** – the manufacturer's liability should continue through the end of the objectively-defined product lifecycle. Additionally, ***Premier recommends that a regulatory process should be established to prohibit medical device manufacturers from receiving approvals for new devices when the manufacturer demonstrates an inability to reasonably maintain cybersecurity levels over a reasonable, objectively-defined lifecycle that is informed by HDO buying patterns.***

Essential to the success of this process is real-world alignment in how a manufacturer and provider define the lifecycle of a type of device or equipment. ***Premier recommends that the FDA leverage RWE to define a data-driven usable lifecycle that aligns with how—and for how long—these products are being used, rather than relying on arbitrary lifecycle estimates from manufacturers that lack data to determine how long they should be required to maintain adequate cybersecurity for the device***. Trusted RWE resources such as the National Evaluation System for Health Technology Coordinating Center (NESTcc) already support the FDA's ability to leverage RWE for medical device evaluation and regulatory decision-making and therefore could also be leveraged for this purpose as well.

In addition, any compliance requirements with cybersecurity requirements should strive to be the least burdensome approach. Given the complexity of interoperable medical devices, and the compliance framework for healthcare overall, it is imperative that FDA work to ensure that future rulemaking and compliance requirements for cybersecurity account for burden on manufacturers and HDOs.

Premier also believes that there should be equitable allocation of fines during a cybersecurity breach. Under current laws and regulations, when a cybersecurity breach does occur, the onus typically falls on the HDO.

These cyberattacks not only threaten patient privacy and clinical safety and outcomes, but also a hospital's financial resources. According to a recent report, the average breach costs in healthcare surpassed $10 million in 2022, with the industry maintaining its top rank for costliest industry breaches for the 12th consecutive year.[1] Alongside direct costs related to a breach, providers may see added costs in hardware, software, firmware and labor.

Premier believes that cybersecurity risk management for medical devices is a shared responsibility among manufacturers and healthcare providers to address patient safety risks and ensure proper device performance. ***Therefore, Premier urges the FDA to create an equitable mechanism for fining HDOs and device manufacturers when a cybersecurity breach does occur based upon the root cause analysis of the incident and commensurate with the findings*.** For example, if a root cause analysis finds that the device manufacturer was primarily at fault for the breach due to a failure to maintain the cybersecurity of their device as defined under this draft guidance, then the manufacturer should be responsible for a majority, if not all, of the associated fines and penalties.

V. CONCLUSION

Premier appreciates the opportunity to comment on the FDA's Select Updates for the Premarket Cybersecurity Guidance. If you have any questions regarding our comments, or if Premier can serve as a resource on these issues to the Administration in its policy development, please contact Mason Ingram, Director of Payer Policy, at Mason_Ingram@premierinc.com or 334.318.5016.

Sincerely,

Soumi Saha, PharmD, JD
Senior Vice President of Government Affairs
Premier Inc.

[1] "Cost of a Data Brach Annual Report." IBM Security, https://www.ibm.com/reports/data-breach 2022