PREMIER TRANSFORMING HEALTHCARE TOGETHER®

October 29, 2023

Kemba Walden
Acting National Cyber Director
Executive Office of the President
1600 Pennsylvania Avenue NW
Washington, DC 20500

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

Re: Request for Information on Cyber Regulatory Harmonization (RIN: 0301-AA00)

Dear Acting Director Walden:

Premier Inc. appreciates the opportunity to submit comments to the Office of the National Cyber Director (ONCD) regarding its request for information (RFI) on opportunities for and obstacles to harmonizing cybersecurity regulations. The RFI is a positive step towards ensuring public engagement in the implementation of the Strategic Objectives of the National Cyber Strategy. Premier supports the ONCD's efforts to combat existing challenges with regulatory overlap and exploration of a framework for reciprocity across regulatory agencies. In our comments, Premier specifically recommends that the ONCD focus on the following:

- 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 that is informed by health delivery organization (HDO) buying patterns;
- Creating resources for HDOs to support decision-making for legacy device risk management, including templates for information-sharing agreements to help set expectations with medical device manufacturers around responsibility and liability for legacy medical devices; and
- Collecting and making publicly available aggregated data on typical costs, quality and security standards, device useful life timelines, etc. to help quantify risks across the healthcare sector, inform policy, and improve alignment of business strategies between HDOs and medical device manufacturers.

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).

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. CYBERSECURITY REGULATION FOR MEDICAL DEVICES

In its RFI, ONCD requests public comment on cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges and priorities, particularly in critical infrastructure sectors and sub-sectors identified in Presidential Policy Directive 21 and the National Infrastructure Protection Plan. 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 Food and Drug Administration (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 month 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.

III. RECENT REGULATORY CHANGES AND ENFORCEMENT CONCERNS

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.

IV. ENSURING CYBERSECURITY OF LEGACY MEDICAL DEVICES

Under current regulatory policy, there are material inconsistencies between the economic useful life of clinical equipment (as measured by the buying patterns of HDOs) and the *supported useful life* of the same equipment as defined by manufacturers. This dynamic creates critical gaps in affordable monitoring and practical management of device life cycle quality and security issues. It is important to note that medical devices that are vulnerable to cybersecurity threats operate in environments that are highly complex from both a technology and policy standpoint. Data is often obtained directly from connected medical devices by multiple vulnerable electronic health record (EHR) systems, and HDOs must manage the transmission of data among intra- and extra provider network applications and devices, many of which are produced by different medical device manufacturers. It is difficult if not impossible for HDOs to ensure reciprocal security and compliance over a device's lifecycle without tools such as structured sBOMs for clinical equipment and devices, inclusive of embedded third-party firmware and software, matched to the HDO's network architecture. It falls to regulatory agencies such as the FDA and federal subject matter experts like ONCD to help ensure that policies are in place to help address these market failures.

V. PREMIER'S RECOMMENDATIONS FOR ADVANCING CYBERSECURITY REQUIREMENTS FOR MEDICAL DEVICES

To address the challenges and gaps described above, Premier recommends that ONCD focus on coordinating across federal partners to advance the following priority areas:

- **Governance.** ***Premier recognizes the strong need for formalized governance frameworks within both HDOs and medical device manufacturers to oversee the medical technology lifecycle.*** Governance within medical device manufacturers should be fully responsible for identifying risks, including cybersecurity risks, throughout the total product lifecycle of medical devices that they place into the market, incorporating an objective definition of the product lifecycle with which HDOs would agree based on the value they derive.

  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.***

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 ONCD work to ensure that future rulemaking and compliance requirements for cybersecurity account for burden on manufacturers and HDOs.

- **Shared responsibility over the medical device lifecycle.** As previously described, 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. ***Premier recommends that ONCD work with federal partners to make resources available to HDOs to support decision-making for legacy device risk management, including templates for information-sharing agreements to help set expectations with medical device manufacturers around responsibility and liability for legacy medical devices.***

- **Objective data collection.** There is a lack of both qualitative and quantitative data to enable HDOs and medical device manufacturers to make informed decisions about the risks and costs of replacement versus the continued use of older-model or legacy medical devices. It is difficult to objectively approach shared responsibility and liability models (as described above) without a reasonable understanding of each other's constraints and baseline standards. ***Premier recommends that ONCD collect and make publicly available aggregated data on typical costs, quality and security standards, device useful life timelines, etc. to help quantify risks across the healthcare sector, inform policy and improve alignment of business strategies between HDOs and medical device manufacturers.***

- **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 ONCD to work with other federal agencies, such as the FDA and Department of Justice (DOJ), and Congress to create an equitable***

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

***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, then the manufacturer should be responsible for a majority, if not all, of the associated fines and penalties.

- **Clarification on cybersecurity requirements for medical devices approved under an emergency use authorization (EUA).** As noted above**,** in the CAA of 2023, Congress required manufacturers of cyber devices to develop processes to ensure their devices are secure, have plans to identify and address cybersecurity vulnerabilities, provide a software bill of materials in their labeling, and submit this information to FDA in any premarket submissions. However, these provisions are only applicable to devices going through a traditional 510(k) pathway and it is unclear how devices and other products granted an EUA during a public health emergency would be required to comply with these provisions. Given heightened cybersecurity concerns during pandemics, ***Premier urges ONCD to work with Congress to clarify the roles and responsibilities of manufacturers granted an EUA as it relates to cybersecurity of their devices.***

VI. CONCLUSION

Premier appreciates the opportunity to comment on ONCD's RFI on cyber regulatory harmonization. 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.