ConnectedHealthInitiative

May 13, 2024

Attn: Dockets Management
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, Maryland 20852

RE: Comments of the Connected Health Initiative regarding *Draft Guidance for Industry and Food and Drug Administration Staff, Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the Federal Food, Drug, and Cosmetic Act* (Docket No. FDA-2021-D-1158)

The Connected Health Initiative (CHI) appreciates the opportunity to provide input on the Food and Drug Administration's (FDA) draft guidance entitled "Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act."[1]

I. Statement of Interest and General Comments of the Connected Health Initiative

CHI is the leading effort by stakeholders across the connected health ecosystem to clarify outdated health regulations, encourage the use of digital health innovations, and support an environment in which patients and consumers can see improvements in their health. We seek essential policy changes that will help all Americans benefit from an information and communications technology-enabled healthcare system. For more information, see www.connectedhi.com.

CHI is a longtime active advocate for the increased use of new and innovative digital health tools in both the prevention and treatment of disease. CHI's advocacy reaches across the divisions of the Department of Health and Human Services, as well as other relevant agencies. In addition, CHI is a member of several related noteworthy efforts and initiatives including being:

- An active member of the Healthcare Sector Coordinating Council.[2]
- An active member of the National Telecommunications and Information Administration's multistakeholder process addressing software component transparency through

[1] 89 FR 18421.

[2] https://healthsectorcouncil.org/

developing solutions to advance the use of software bills of materials (SBOMs) widely – notably, this effort has a working group dedicated to addressing healthcare SBOMs.[3]

Connected medical devices are radically improving the American healthcare system and will continue to do so. Mobile-app enabled telehealth and remote monitoring of patient-generated health data continues to represent the most promising avenue for improved care quality, reduced hospitalizations, avoidance of complications, and improved satisfaction, particularly for the chronically ill.

While the rise of the internet of things (IoT) via internet protocol-enabled products (including medical devices) holds great promise, this environment also faces increasing security threats due to a broadened attack vector, necessitating more evolved and dynamic risk management practices. No data is more personal to Americans than their health data. CHI members appreciate this and put extensive resources into ensuring the security and privacy of sensitive health data to earn and maintain the trust of consumers, hospital systems, and providers.

We acknowledge the FDA's leadership and work to provide clarity and guidance regarding cybersecurity vulnerabilities in the pre-market context. We support the FDA's efforts to build on the voluntary, flexible, and scalable National Institute of Standards and Technology Cybersecurity Framework (NIST Cybersecurity Framework) risk management tool,[4] which has promoted a harmonized approach to cybersecurity risk management for critical infrastructure, further supplemented in the medical device context by standards. Further, CHI agrees with the FDA that "security-by-design"—the concept of building security concepts into hardware and software from the developmental stages to the "end of life"—is a cornerstone of protecting patient safety in this new landscape. Building on our broad support for the FDA's continued work to improve cybersecurity risk management for medical devices, we offer the following general input:

- CHI recommends that FDA fully incorporate its updates into the existing Premarket Cybersecurity guidance, rather than appending these updates as new section. Such an approach will ensure that new updates are fully appreciated by all relying on the guidance, and reduce any confusion related to updated guidance.
- CHI continues to support the FDA's advancement of risk-based design and validation, which should ensure that medical devices can be designed with appropriate security depending on the feature and risk posed, rather than a one-size-fits-all approach, consistent with the NIST Cybersecurity Framework. We encourage maximum alignment with the single risk approach put forward by FDA in its guidance on post-market cybersecurity.

  We encourage FDA to ensure that its guidance on premarket submissions for device

[3] https://www.ntia.doc.gov/SoftwareTransparency

[4] https://www.nist.gov/cyberframework.

software functions reflects that the level of substance and detail in premarket documentation is scaled to the risk posed by the device software function (and not the intended use of either the device software function or the entire device that includes the device software function). Further, a modified version of a previously cleared or approved device that has undergone one or more non-significant changes to software functions since an earlier approval or clearance may not require full re-testing. Such an approach would ensure consistency with FDA's general approach to digital health and risk management as well as key U.S. government policies FDA has long sought to align with such as the NIST Cybersecurity Framework risk management tool, and relevant standards including IEC 62304 (Medical Device Software – Software Life Cycle Processes)[5] and ANSI/AAMI/ISO 14971 (Medical devices – Application of risk management to medical devices).[6]

Accordingly, FDA's proposed levels of documentation in the Guidance should follow this risk-based and scaled approach (and avoid, for example, requiring enhanced documentation for a software device function that is part of a larger medical device which may pose higher risk to a patient despite that software function having no role in creating that higher risk). FDA should ensure that its guidance does not result in excessive and unnecessary documentation requirements that would do little to provide for patient safety. Documentation requirements should also map to standardized approaches, including ANSI/AAMI/IEC 62304:2006/A1:2016 (with the FDA has already recognized as a consensus standard).

- The voluntary timely sharing of cybersecurity threat indicators among stakeholders from both the public and private sectors will be crucial in the detecting, mitigating, and recovery of cybersecurity threats. CHI agrees with the FDA on the key role of information sharing in cybersecurity risk management and supports the role of information sharing and analysis organizations (ISAOs) in addition to valuable information sharing and analysis centers (ISACs). We support FDA's partnership with the National Health Information Sharing and Analysis Center (NH-ISAC), and in the memorandums of understanding it has reached with MedISAO and Sensato-ISAO. The rise of ISAOs as a complement to ISACs helps to address the resource limitations of small and medium-sized businesses as well as the convergence of business models that may make it difficult to determine which ISAC to engage. CHI supports FDA's efforts to facilitate the timely sharing of cybersecurity threat information in the Draft Guidance.

[5] https://www.iso.org/standard/38421.html.

[6] https://webstore.ansi.org/standards/aami/ansiaamiiso149712019.

- CHI agrees that software bills of materials (SBOMs) can and should be a valuable tool in identifying assets, threats, and liabilities. We appreciate FDA's alignment of its own terminology to use the term SBOM (rather than the previously proposed term cybersecurity bill of materials (CBOMs)) to reduce uncertainty. Further, we recommend that the definition of a SBOM should clarify for the stakeholder community that it need not contain proprietary information (e.g., code). Further details around the FDA's proposal to require a SBOM should also be provided, such as what developments should merit the SBOM to be updated for end users. CHI recommends that FDA align its approach to SBOMs with the product of the NTIA multistakeholder effort, and that FDA's approach to SBOMs stay consistent with industry standards and the NTIA specification of minimum SBOM elements.
- In providing education on cybersecurity and the risks associated with using technologies, vendors and manufacturers should explain why technologies need to be updated in plain English, using standardized formats, and with a consistent articulation of level of risk, along with information on how to identify the altered performance of devices. Cyberattacks may change the normal function of a device and, without knowing what to look out for, providers may not know when a product is malfunctioning. This is particularly important when providers rely on data from medical devices to monitor or treat patients. When a vulnerability or threat is detected, such information should be communicated in an easily understood and automated manner to the greatest extent practicable so that the level of risk is identified and articulated through the concept of patient safety where possible (as physicians respond strongly when cybersecurity is viewed through this lens), and should also include specific steps to address vulnerabilities. As described above, providers also need to understand what software and hardware exist within their medical technologies using a SBOM.

II. Specific Comments of the Connected Health Initiative on the FDA's Draft Updates to its Premarket Cybersecurity Guidance

CHI offers the following specific inputs on the FDA's proposed updates to its Guidance:

- Definitional clarifications:
    - In lines 64-68, CHI requests that FDA clarify that a "cyber device" under 524B(c) depends on meeting all three prongs under this section and provide further key examples.
    - At line 67, CHI requests further clarification and examples to support broader understanding of the intentional versus unintentional inclusion in a product.
    - In its discussion of coordinated vulnerability disclosures at lines 104-105, CHI requests that FDA tie in both its guidance for off-the-shelf software as well as

AAMI CR510 (Appropriate Use of Public Cloud Computing for Quality Systems And Medical Devices).[7]

- At lines 112-116, CHI urges FDA to defer to its examples of vulnerabilities that must be remediated and responded to because of the risk of patient harm in its existing guidance for postmarket cybersecurity guidance, or to at least provide further examples of appropriate and reasonable justifications for developing and releasing required updates and patches. Without further description and examples from FDA, we are concerned that those relying on the guidance would be left to make too subjective a determination.
- At lines, 130-136, CHI urges FDA to define the term "risk profile" to harmonize understanding across the communities relying on this guidance and related underlying standards (where the term is not defined).
- At lines 143-150, CHI requests clarifying language as to what "related systems" and "other functions" that the FDA considers in scope.
- At lines 146-147, CHI requests FDA clarification as what is meant by "connections to health care facility networks," and to what degree remote connection-facilitated updates/servicing is included in scope.
- At likes 174-183, we urge FDA to, rather than create a new category for cyber category fully integrate, and where appropriate build on, its guidance updates into existing clarifications provided in existing premarket cybersecurity guidance on security architecture and security controls.

- At lines 154-157, CHI notes its support for FDA's support for the use of SBOMs, and requests further coordination and alignment with the Department of Homeland and Security's leading SBOM work.[8]

[7] https://array.aami.org/doi/book/10.2345/9781570208225.

[8] https://www.cisa.gov/sbom.

III. Conclusion

CHI appreciates the opportunity to submit its comments to the FDA and urges its thoughtful consideration of the above input.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005