ConnectedHealth

March 18, 2019

Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, Maryland 20852

RE: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability *(Docket No. FDA-2018-D-3443)*

The Connected Health Initiative (CHI) appreciates the opportunity to provide input on the Food and Drug Administration's (FDA) draft guidance addressing the content of premarket submissions for management of cybersecurity in medical devices.[1]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CHI is the leading effort by stakeholders across the connected health ecosystem to clarify outdated health regulations, encourage the use of digital health innovations, and support an environment in which patients and consumers can see improvements in their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 American healthcare system. For more information, see www.connectedhi.com.

[1] https://www.regulations.gov/document?D=FDA-2018-D-3443-0001.

CHI is a long-time 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. CHI is a member of several related noteworthy efforts and initiatives including:

- CHI a board member of Xcertia, a collaborative effort to develop and disseminate mHealth app guidelines that can drive the value mHealth apps products bring to the market and the confidence that physicians and consumers can have in health apps and their ability to help people achieve their health and wellness goals.[2]
- CHI is an active member of the Healthcare Sector Coordinating Council.[3]
- CHI is an active member of the National Telecommunications and Information Administration's multistakeholder process addressing software component transparency through 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.[4]

Connected medical devices are radically improving the American healthcare system and will continue to do so. Global consumers spend in Health and Fitness apps have grown 3x in 2018 from 2016.[5] 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 own 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.

[2] http://www.xcertia.org/

[3] https://healthsectorcouncil.org/

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

[5] http://www.netimperative.com/2019/01/the-state-of-mobile-in-2019-app-spend-worth-double-box-office-market/.

We acknowledge the FDA's leadership and work to provide clarity and guidance regarding cybersecurity vulnerabilities in the post-market context. We support the FDA's efforts to build on the voluntary, flexible, and scalable National Institute of Standards and Technology Cybersecurity Framework risk management tool (NIST Cybersecurity Framework),[6] which has promoted a harmonized approach to cybersecurity risk management for critical infrastructure, further supplemented in the medical device context by standards like ANSI/AAMI/ISO 14971:2007/(R)2010, Medical devices – Application of risk management to medical devices. Further, the 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.

II. Specific Comments of the Connected Health Initiative on the FDA's Draft Guidance

Building on our broad support for the FDA's continued work to improve cybersecurity risk management for medical devices, we offer the following specific input:

- CHI supports 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. The approach put forward by FDA in the draft guidance that would create a new two-tiered risk framework which, as the FDA notes, "may not track to FDA's existing statutory device classifications" while still being consistent with the NIST Cybersecurity Framework.[7] We are concerned that this new two-tiered approach to risk classification would introduce uncertainty for cutting edge medical devices due to its departure from the single risk approach put forward by FDA in its guidance on post-market cybersecurity. CHI therefore requests that FDA discard its proposed two-tiered risk-based approach in the Draft Guidance and utilize a single-tiered risk-based approach consistent with its approach taken in the context of cybersecurity in the post-market context.

[6] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[7] Draft Guidance at pgs. 10-11.

- 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 entities 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.
- CHI agrees that cybersecurity bills of materials (CBOMs), defined as "a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities," when shared with end users, can be a valuable tool in identifying assets, threats, and liabilities. We do note that the term SBOM is already used and is more widely understood (e.g., the NTIA multistakeholder effort on software transparency noted above that the CHI is a participant in) and suggest that FDA align its own terminology in the Draft Guidance to use the term SBOM rather than CBOM to reduce uncertainty. Further, we recommend that the definition of an SBOM (or CBOM, if such terminology is retained by FDA nonetheless) 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/CBOM should also be provided, such as what developments should merit the BOM to be updated for end users. Because many of these details are currently being addressed in the NTIA effort discussed above, CHI believes it would be wise for FDA to allow the NTIA process to complete, and then align its approach to SBOMs/CBOMs with the product of the NTIA multistakeholder effort.
- 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 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.

- CHI appreciates FDA's efforts to address labeling in the Draft Guidance, but we urge FDA to give careful consideration to whether each of the 14 categories of information to be included in a label for cybersecurity purposes is reasonably related to intended usual uses. Some of the cybersecurity information proposed for inclusion in labeling in the Draft Guidance is likely more appropriate to be recommended for inclusion in communicated information, rather than in labeling, such as a CBOM.

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

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