HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership

December 17, 2020

Division of Dockets Management (HFA –305)
Food and Drug Administration
5630 Fishers Lane - Room 1061
Rockville, MD 20852

Via www.regulations.gov

RE: Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework
[Docket FDA-2020-N-1933]

Dear Sir or Madam:

The Health Sector Coordinating Council ("HSCC") appreciates the opportunity to provide input on the Food and Drug Administration's ("FDA") Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework, Discussion Paper and Request for Feedback ("Framework").

The HSCC is a private sector-led critical infrastructure advisory council of large, medium and small health industry stakeholders working with government partners to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to our nation's citizens. The HSCC participates in the Critical Infrastructure Partnership Advisory Council and works closely with the Department of Health and Human Services as the Sector Specific Agency for the Healthcare and Public Health Sector. A major component of the HSCC is its Cybersecurity Working Group, which represents 300 healthcare organizations in the subsectors of direct patient care, medical materials, health information technology, health plans and payers, laboratories, biologics and pharmaceuticals, and public health. Our members collaborate toward improving the cyber security and resiliency of the healthcare industry and patient safety.

Sharing and communication of cybersecurity vulnerability information among healthcare stakeholders is critical to enabling the healthcare sector to effectively and efficiently identify, respond to, and mitigate cybersecurity vulnerabilities in medical technology. Accordingly, in October 2019 HSCC and its members created the MedTech Vulnerability Communications Task Group (VCTG). The VCTG was launched in 2020 to evaluate the challenges of medical technology vulnerability communications and make recommendations to improve communication consistency, efficiency, and effectiveness. The VCTG is co-chaired by Abbott, Fresenius Medical Care, and FDA CDRH, and is composed of approximately 60 members from a diverse group of healthcare organizations including medical device manufacturers, healthcare delivery organizations, federal agencies, and cybersecurity solutions companies.

During 2020 the VCTG held a series of webinars with key stakeholder groups to better understand the current state of medical device vulnerability communications and identify opportunities for improvement. These stakeholders included the Department of Homeland Security, physicians, healthcare delivery organizations (HDOs), security researchers, media, and medical device manufacturers. We obtained valuable insights into the state of vulnerability communications in healthcare through these discovery sessions, including:

- **Diverse stakeholders with diverse needs –** Many stakeholder groups within healthcare interact with and rely on medical technology. Their needs and understanding concerning cybersecurity vulnerability information vary based on their role. Stakeholder groups include physicians and clinical support staff, HDO information technology and security teams, and most importantly, patients and caregivers. Cybersecurity vulnerability information must be communicated to each of these groups in a way that is understandable and actionable to facilitate a timely response, while adequately balancing the cybersecurity risks and benefits of the medical technology. For patients and caregivers, this includes appropriately framing patient safety risks.
- **Expanding technology environment –** The types of devices and how they interact with the healthcare ecosystem is changing faster than ever. Approaches for vulnerability communications vary based upon the type of device, the device's technical capabilities, primary users, and intended use - among other factors. New technologies are constantly being introduced and the demand by patients for consumer technology means it is more critical than ever to engage patients in vulnerability communications.
- **Cybersecurity complexity –** Understanding cybersecurity vulnerabilities, how they can be exploited, the impact on the device, and mitigation approaches is often highly technical and complex. Ensuring communications are clear, concise, and understandable for their intended audience is critical to ensuring a timely and effective response.

Through the leadership of the VCTG, the HSCC appreciates FDA's efforts to develop and release the Framework for stakeholder feedback. HSCC would like to provide and continue to work with FDA on several specific considerations, including:

- **Balance timeliness with risk:** HSCC agrees that timely communication is critical; however, consideration should be made for when a vulnerability is not widely known and the risk of revealing the information prior to an available patch may introduce additional risk.
- **Accommodate timely multilingual communications**: Ensuring availability of information to ESL audiences who prefer reading in their native language is an important goal for any vulnerability communication. However, translated messaging should be communicated to the appropriate audience as it becomes available and not held until all versions are complete, particularly for urgent communications. Efforts should be made to ensure timely translation.
- **Put recommended actions up front**: It would be beneficial to highlight recommended actions at the beginning of any communication to ensure the readers understand actions they should take. A specific named section for recommended actions would aid in this goal.

- **Make Communications Easy for Patients to Find and Use:** FDA could also provide overall instructions/training to patients and caregivers, including pointers to medical device manufacturers' website security pages.

The FDA's Framework, along with the feedback obtained through the stakeholder research described above, provides a basis for the VCTG recommended next steps, which include:

- **Patient-Focused Glossary of Terms –** Communicating complex cybersecurity and technical concepts to diverse patient populations in a manner that facilitates understanding and a timely response is critical. The VCTG plans to develop a patient-focused glossary of terms, which can be used by stakeholders developing patient-focused communications to ensure they are using the most effective terminology. Over time our goal is to increase patient cybersecurity literacy to improve the effectiveness of these communications.
- **Sample Vulnerability Communications –** Develop sample vulnerability communications for different types of medical technology and vulnerability scenarios that can be used as references or templates for organizations when developing patient-focused communications.
- **Message Effectiveness Standards –** Develop standards and best practices for measuring the effectiveness of patient-focused cybersecurity communications. These standards will allow the industry to compare various communication approaches and support ongoing continuous improvement efforts.

Given the complexities of vulnerability communication and the continually evolving technology and cybersecurity landscape, more work will be needed far beyond this initial set of focus areas. We recommend that FDA continue to collaborate with multi-stakeholder groups like the HSCC to develop such implementation tools to provide additional guidance to the industry and drive consistency for patients and other healthcare stakeholders. Such collaboration will allow for quicker and more frequent updates to existing tools and the development of new tools based on evolving technology and cybersecurity environments while incorporating feedback from previous efforts and communications. This includes developing processes to perform regular updates to patient communications when required as information related to a specific vulnerability can change over time with respect to risks and recommended responses.

The HSCC would like to thank the FDA for its consideration of these comments and looks forward to working with the FDA on this critical area.

Respectfully submitted,

Greg Garcia

Greg Garcia
Executive Director, Cybersecurity
Health Sector Coordinating Council