799 9th Street NW
Suite 210
Washington, DC 20001

T (202) 354-2600
vizientinc.com

March 18, 2019

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

Commissioner Scott Gottlieb, M.D.
Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 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Re: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff; Availability [Docket No. FDA–2018–D–3443]

Dear Dr. Gottlieb:

Vizient, Inc. respectfully submits our comments to The Food and Drug Administration (FDA or the Agency) regarding the "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices; Draft Guidance for Industry and Food and Drug Administration Staff" as published on October 18, 2018 in the Federal Register (Vol. 83, No. 202).

Background

Vizient is the nation's largest health care performance improvement company. Our mission is to strengthen our members' delivery of high-value care by aligning cost, quality and market performance. Vizient is member-driven and member-minded, working tirelessly to amplify each organization's impact by optimizing every interaction along the continuum of care. We serve a diverse membership including academic medical centers, pediatric facilities, community hospitals, integrated health delivery networks and non-acute health care providers. Vizient is headquartered in Irving, TX with locations in Chicago, Washington, D.C., and other cities across the country.

Recommendations

Vizient appreciates The Food and Drug Administration's continued focus on medical device cybersecurity. We are committed to minimizing the risk and cost of medical device cybersecurity by fostering standard practices for the benefit of the health care industry. Vizient supports the FDA's proactive approach to update guidance with recommendations to consider and information to include in medical device premarket submissions for effective cybersecurity management.

We would like to thank the FDA for holding the public workshop on January 29 and 30, 2019 with a group of diverse stakeholders – including Vizient – to discuss, in-depth, the draft guidance. Vizient appreciated the opportunity to discuss the subtopic of the draft guidance regarding a Cybersecurity Bill of Materials (CBOM), which we agree can be a critical element in

identifying assets, threats, and vulnerabilities. We offer our further recommendations regarding a CBOM below.

Ensuring alignment with rapid technology advancement while determining whether the benefit outweighs the risk for a new device is only made more complex with the ever-changing cybersecurity threats present in today's health care landscape. We applaud the Agency's efforts in continuing to foster innovation, while adapting processes and programs to keep pace with technology advancement. We recognize the challenges that accompany the crucial role that the Agency plays in regulating these devices, and are committed to working with the FDA to achieve effective cybersecurity and assure medical device functionality and safety. Vizient thanks the FDA for the opportunity to share our input and recommendations regarding how the Agency can assist the device industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices.

Vizient agrees with the Agency that an updated approach on guidance addressing recommendations for device cybersecurity information in premarket submissions is needed due to the rapidly evolving landscape, and the increased understanding of the threats and their potential mitigations. Vizient appreciates the draft updates to the existing "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" guidance. Vizient is working to better protect our members against cybersecurity risks – such as ransomware campaigns – that could disrupt clinical operations, delay patient care, and possibly harm patients. As a member-driven, performance improvement company, we strongly support policies that would enhance the ability of hospitals throughout the country to deliver safe and effective health care.

General Principles & Risk Assessment

Vizient supports the FDA's approach in defining two "tiers" of devices according to their cybersecurity risk, and agrees that this will clarify the Agency's premarket cybersecurity recommendations. However, we urge the FDA to consider broadening the criteria for Tier 1 "higher cybersecurity risk" devices. According to the draft guidance, a "device is a Tier 1 device if the following criteria are met: 1) the device is capable of connecting (e.g., wired, wirelessly) to another medical or non-medical product, or to a network, or to the Internet; and 2) a cybersecurity incident affecting the device could directly result in patient harm to multiple patients." Vizient urges the FDA to modify the definition under the second criteria so that it reads "a cybersecurity incident affecting the device could directly result in patient harm" thus removing the requirement that the device impact multiple patients in order to be considered high risk. It is critical that device manufacturers adhere to the highest possible standards, so that any patient harm would indicate a higher cybersecurity risk.

Hospitals and health care systems continue to struggle with independently assessing the cybersecurity risk level of medical devices. Furthermore, devices may be connected to multiple systems and applications, increasing the chances where a threat may enter their network undetected. Vizient members are exceedingly dedicated to reducing preventable harm, making care safer, and encouraging the highest-quality care. Patient safety – not just for all or some patients, but for each individual patient – is of the utmost importance for hospitals and health systems.

Designing a Trustworthy Device: Application of NIST Cybersecurity Framework

In order to protect and promote public health and patient safety while encouraging innovative devices that provide clinical benefit, both providers and device manufactures must promote and

prioritize cybersecurity. Vizient supports the FDA's application of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. We appreciate the recommendations to require documentation demonstrating the trustworthiness of a device, which will help the Agency more quickly and efficiently assess the device's safety and effectiveness with respect to cybersecurity. Vizient is strongly supportive of the FDA's recommended specific design features and cybersecurity design controls that should be included in the design of a trustworthy device. Purchasing and utilizing trustworthy devices will in turn encourage and empower providers in their ability to provide health care security.

Identify and Protect Device Assets and Functionality

Vizient agrees with the FDA that manufacturers should design trustworthy devices and provide documentation to demonstrate the trustworthiness of their devices in premarket review, and supports the protection mechanisms recommended. Furthermore, Vizient agrees that manufacturers should ensure the confidentiality of any/all data whose disclosure could lead to patient harm. We support the provided design recommendations with respect to authentication, authorization, and encryption. Additionally, we recommend including a reference to NIST Digital Identity Guidelines.

Maintain Confidentiality of Data

As the Agency notes, harms such as loss of confidential protected health information (PHI), are not considered "patient harms" for the purposes of this guidance, and protecting the confidentiality of PHI is beyond the scope of the guidance. Furthermore, manufacturers and/or other entities may be obligated to protect the confidentiality, integrity, and availability of PHI throughout the product lifecycle in accordance with applicable federal and state laws – including the Health Information Portability and Accountability Act (HIPAA)[1]. However, Vizient would like to note that there are instances where a compromise to the integrity and availability of PHI or device data could cause patient harm. For example, if a patient's blood type is changed or unavailable, or if the formulary of a drug being administered (e.g., information stored on a device) was altered.

Labeling Recommendations for Devices with Cybersecurity Risks

Vizient appreciates the FDA's labeling recommendations for communicating relevant security information to end-users that may help manufacturers comply with applicable requirements and help ensure a device remains safe and effective throughout its life-cycle. The sharing of key information by device vendors greatly assists in assessing the risk level and potential mitigations. Vizient agrees with the FDA's recommendation that when drafting labeling for inclusion in a premarket submission, a manufacturer should consider all applicable labeling requirements and how informing users through labeling may be an effective way to manage cybersecurity risks. Vizient further encourages the FDA to consider categorizing the labeling recommendations for devices with cybersecurity risks under a separate category with a security implementation guide, which could include all necessary device cybersecurity configuration and operations information. This would make it easier for health industry professionals to communicate these requirements.

Cybersecurity Bill of Materials

Vizient is encouraged that the FDA is seeking feedback on a Cybersecurity Bill of Materials (CBOM). Vizient supports the Agency in the development of a CBOM that would be provided to the FDA as part of a premarket submission and made available to medical device customers

[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Pub. L. 104-191.

and users. This will greatly benefit our provider members, as customers and users by enabling them to better manage their networked assets, and be aware of which devices in their inventory or use may be subject to vulnerabilities.

We broadly agree with the definition of CBOM that the Agency has recommended. Vizient strongly believes that a CBOM should include both software and hardware information. For example, there have been a number of vulnerabilities in both central processing units (CPUs), as well as wireless chipsets. Therefore, we encourage the FDA to recommend that these higher-risk hardware components are disclosed in a CBOM in order to better allow health care delivery organizations to assess the device's risk based on known hardware vulnerabilities. Device transparency is vital to the governance of medical devices within the walls of a hospital, and furthermore brings awareness to any vulnerabilities that may require patching or segmentation post-implementation. This information can assist in reducing vulnerabilities by which a threat may enter their network undetected – which is essential for all hospitals and health systems.

End of Support Considerations

Vizient appreciates and fully supports the labeling recommendation for information, if known, concerning device cybersecurity end of support. At the end of support, a manufacturer may no longer be able to reasonably provide security patches or software updates. Vizient agrees that if the device remains in service following the end of support, the cybersecurity risks for end-users can be expected to increase over time. Therefore, we strongly support this recommendation and agree with the FDA that communicating relevant security information to end-users will help to ensure a device remains safe and effective throughout its life-cycle.

Even with advances in medical device cybersecurity, over time, many new devices will still fall into the "legacy" category with unsupported software components. Vizient urges the FDA to consider requesting manufacturers include the expected lifespan of their device (i.e., planned end of support date), as well as any relevant information regarding support for the product during this lifespan (e.g., operating software (OS) upgrades). This information will provide health care delivery organizations with important information needed to make informed purchasing decisions. Furthermore, it will allow suppliers to provide better estimates of the full cost of a device throughout its total produce life cycle (TPLC).

Final Comments and Recommendations

Vizient looks forward to working with the Agency and other health care stakeholders on an agreed upon set of cybersecurity best practices. Last year, Vizient launched the Medical Device Cybersecurity Task Force which is now a permanent Vizient council, and includes information security leaders from 25 of our member health system organizations. Because of our relationship with thousands of suppliers, hospitals, and health systems, Vizient is uniquely positioned to bring these experts together to facilitate a path to enhance security. This path requires a group effort – members, suppliers and industry experts – working together on solutions. Vizient's contract portfolio includes more than 500 contracts with networked devices and we are working closely with members, suppliers and cybersecurity experts to add additional terms into the contract language as well as modifications to the weightings related to cybersecurity safeguards in our Request for Proposal (RFP) scoring process. This will enhance the cybersecurity of the devices in Vizient's portfolio – ultimately benefitting both patients and providers.

Conclusion

Vizient welcomes the FDA's discussion and its emphasis on stakeholder involvement, which provides a significant opportunity for the health care industry to inform the Agency on assisting the device industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices.

We look forward to continuing to work with the FDA to assure patients and providers have access to the information they need across the Total Product Life Cycle of a device by leveraging the full range of the Agency's premarket and postmarket expertise, data, knowledge, and tools at all stages of a device's development, evaluation, and marketing. Vizient encourages and supports the direction that the FDA has taken to deliver a robust medical device patient safety net, and looks forward to providing continued feedback and support.

Vizient membership includes a wide variety of hospitals ranging from independent, community-based hospitals to large, integrated health care systems that serve acute and non-acute care needs. Additionally, many are specialized, including academic medical centers and pediatric facilities. Individually, our members are integral partners in their local communities, and many are ranked among the nation's top health care providers.

In closing, on behalf of Vizient, I would like to thank the FDA for providing us this opportunity to comment on this important proposal. Please feel free to contact me at (202) 354-2600 or Chelsea Arnone, Director of Regulatory Affairs and Government Relations (chelsea.arnone@vizientinc.com), if you have any questions or if Vizient can provide any assistance as you consider these issues.

Respectfully submitted,

Shoshana Krilow
Vice President of Public Policy and Government Relations
Vizient, Inc.

cc: Jeffrey E. Shuren, M.D., J.D.
Suzanne B. Schwartz, M.D., M.B.A.