December 14, 2018

Dr. Scott Gottlieb, M.D.
Commissioner
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

Re: Support of the Medical Device Safety Action Plan

Dear Commissioner Gottlieb,

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to support the Food and Drug Administration's (FDA) Medical Device Safety Action Plan released on April 17, 2018. This critical document is an indication of the agency's recognition that cybersecurity threats associated with medical devices can pose risks to patient safety. This document represents a strong step toward enhanced cybersecurity preparedness, resilience and response across the healthcare sector, ensuring that medical device cybersecurity is a truly shared responsibility among industry stakeholders.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), and other senior healthcare IT leaders. Consisting of more than 2,800 members in 51 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 875 chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members take their responsibility to protect the privacy and security of patient data and devices networked to their system very seriously. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topic of cybersecurity.

In an era of increasingly ubiquitous device connectivity ranging from the Internet of Things (IoT) devices to the quest for nationwide interoperability, cybersecurity threats have grown at a rapid pace with increased severity. We welcome the FDA laying out in this blueprint a way to address a myriad of concerns we have raised to the agency over the past several years, and as noted above, we are especially pleased to see the focus on patient safety. These include: a more robust premarket process; possible new postmarket authorities; and the development of a CyberMed Safety (Expert) Analysis Board (CYMSAB), a public-private partnership that could be leveraged by device manufacturers and the agency to improve patient safety of medical devices. Furthermore, we are pleased to see the FDA acting on some of the recommendations made in the Health Care Industry Cybersecurity Task Force report published in June 2017 around improving device security.

Specifically, we support the agency acting on their intention to publish updated premarket guidance, including the "Software Bill of Materials" component. Providers managing cyber risks and vulnerabilities across several interconnected medical devices need this information at the time of purchase as it is critical in order to maintain strong resiliency. We plan to submit additional comments specifically on the proposals included in the draft "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." We also appreciate that the FDA is hosting a summit to address the issues raised in draft premarket guidance and other related policies in January. Lastly, we welcome and support the concept of the CYMSAB and recognize the need for full funding for FDA to operationalize this entity. FDA says this new body's "functions would include assessing vulnerabilities,

evaluating patient safety risks, adjudicating disputes, assessing proposed mitigations, serving in a consultative role to organizations navigating the coordinated disclosure process, and serving as a 'go-team' that could be deployed in the field to investigate a suspected or confirmed device compromise *at a manufacturer's or FDA's request*" (emphasis added). We thank the agency for actively seeking our input into the formation of this new body and look forward to supporting provider input and representation when it is stood up. We respectfully request: 1) provider representation on this body; and 2) that providers be able to request investigation into a suspected or confirmed compromise.

Last, we recognize that the FDA's vision for medical device safety is aimed at protecting patients and spurring innovation of new products that are safer, more effective, and address unmet medical needs. To that end, part of the agency strategy for modernizing the FDA's approach to device safety includes the agency's National Evaluation System for Health Technology (NEST) effort which incorporates pilot testing using real world data. FDA has said, "The promise of NEST is clear: real-time device safety information means better outcomes for patients who depend on devices to improve their health." In the agency's *Developing Software Precertification Program: A Working Model* (v0.2 – June 2018), the FDA lays out their concept for precertification of software manufacturers "who have demonstrated a culture of quality and organizational excellence and would leverage data from all appropriate sources." CHIME and AEHIS are pleased to see that among the five principles upon which the agency would evaluate organizational excellence is "cybersecurity responsibility," which the FDA says is, "Demonstration of excellence in responsibly conducting clinical evaluation and ensuring that patient-centric issues, including labeling and human factors, are appropriately addressed." It is unclear to us to what degree cybersecurity experts have been included in these efforts and we welcome the chance to aid with this effort.

CHIME and AEHIS are pleased to see FDA's increased attention to the cybersecurity of medical devices. We welcome the opportunity to share our members' perspective and we appreciate your attention to this important issue. Should you have any questions or if we can be of assistance, please contact Mari Savickis, Vice President of Federal Affairs, at Mari.Savickis@chimecentral.org.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Erik Decker
Chair, AEHIS Board
CISO and Chief Privacy Officer
University of Chicago Medicine