April 1, 2019

The Honorable Nita Lowey
Chairwoman
Committee on Appropriations
United States House of Representatives
Washington, DC 20515

The Honorable Kay Granger
Ranking Member
Committee on Appropriations
United States House of Representatives
Washington, DC 20515

The Honorable Sanford Bishop
Chairman
House Subcommittee on Agriculture, Rural Development, Food and Drug Administration and Related Agencies
United States House of Representatives
Washington DC, 20515

The Honorable Jeff Fortenberry
Ranking Member
House Subcommittee on Agriculture, Rural Development, Food and Drug Administration and Related Agencies
United States House of Representatives
Washington DC, 20515

Re: Support Letter for FDA Cybersecurity Funding and Authority

Dear Chairwoman Lowey, Ranking Member Granger, Chairman Bishop and Ranking Member Fortenberry,

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) appreciates the inclusion of language in the Food and Drug Administration's (FDA) fiscal year 2020 justification of estimates for the appropriations committees that acknowledges of their lack of authority to regulate the cybersecurity of medical devices. We appreciate the FDA's interest in ensuring lifesaving medical devices are secured and welcome the opportunity to offer perspective from our members, the nation's healthcare chief information officers (CIOs) and chief information security officers (CISOs).

CHIME is an executive organization that serves more than 2,800 CIOs and other senior health information technology leaders across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. CHIME members are among the nation's foremost health IT experts on a wide range of topics, including cybersecurity. Within CHIME is AEHIS, an organization launched in 2014 which represents more than 850 CISOs and provides education and professional development for senior IT security leaders in healthcare. CHIME and AEHIS members take very seriously their responsibility to protect the privacy and security of patient data and devices networked to their systems.

Healthcare has entered an era of ubiquitous connection, and the internet of things (IoT) is transforming healthcare along with the world's economy. Tens of thousands of medical devices can be used throughout large healthcare systems, many of which are connected directly to the patient or serving to provide information to inform clinical decision making. Wearables and medical devices are

being directly connected to electronic health record (EHR) systems, which generates additional data for clinical decision making but also increases the threat surface.

To "Transform Medical Device Safety, Cybersecurity, Review, and Innovation" FDA has requested $55 million which includes the creation a cybersecurity unit to complement the advances in software-based devices as well as to aid in review of cybersecurity advances affecting the more traditional, hardware and software-based medical devices. The FDA budget justification states:

> *"Currently, there is no statutory requirement (pre- or post-market) that expressly compels medical device manufacturers to address cybersecurity. This proposal would advance medical device safety by ensuring FDA and the public have information about the cybersecurity of devices. Specifically, FDA seeks to require: that devices have the capability to be updated and patched in a timely manner; that premarket submissions to FDA include evidence demonstrating the capability from a design and architecture perspective for device updating and patching; a phased-in approach to a Cybersecurity Bill of Materials (CBOM), 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; and that device firms publicly disclose when they learn of a cybersecurity vulnerability so users know when a device they use may be vulnerable and to provide direction to customers to reduce their risk. The proposal also seeks to improve proactive responses to cybersecurity vulnerabilities."*[1]

Cybersecurity incidences like Petya and WannaCry demonstrated how vulnerable some network connected devices can be, thus we support the FDA's efforts to secure the healthcare sector. As the FDA states, "Newer devices are more often interconnected and interoperable, increasing cybersecurity threats." Viewing security as a component of safety and efficacy of device functions and embracing "security by design" are necessary to keep pace with these variable threats. A secure healthcare system will ultimately enable greater consumer confidence and will spur better care coordination, enhanced information exchange and improved patient care.

We applaud the Devices Program's goal to encourage a coordinated approach of vigilance, responsiveness, resilience, and recovery with respect to cybersecurity that fits the culture of continuous quality improvement. The FDA states that this equates to taking a total product lifecycle approach, starting at the product design phase when FDA builds in security to help foil potential risks, followed by having a plan in place for managing any risks that might emerge, and planning for how to reduce the likelihood of future risks. Specifically, FDA states that medical device manufacturers are encouraged to proactively update and patch devices in a safe and timely manner. The concept of updates and patches, while not new to traditional information technologies, is complex when it comes to critical safety systems and requires a collaborative approach to finding solutions. FDA has published guidance documents – recommendations for manufacturers and others – that contain recommendations for comprehensive management of medical device cybersecurity risks throughout the total product life cycle. This includes closely monitoring devices already on the market for cybersecurity issues. To enable more expedient actions, the Devices Program's overall approach incentivizes industry to make changes to marketed and distributed medical devices to reduce risk.

[1] Department of Health and Human Services Fiscal Year 2020 Food and Drug Administration Justification of Estimates for Appropriations Committees, Available at: https://www.fda.gov/downloads/AboutFDA/ReportsManualsForms/Reports/BudgetReports/UCM633738.pdf

Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. This vulnerability increases as medical devices are increasingly connected to the Internet, hospital networks, and other medical devices, and as patient demand greater access to their information in more nimble ways like via application programming interfaces (APIs) on third party mobile apps. In recent years, FDA, manufacturers, and healthcare entities have made tremendous strides to improve the cybersecurity of medical devices.

The requested FDA authority and funding detailed in the budget justification would be an integral step in ensuring that all stakeholders understand what is necessary to contribute to the shared responsibility of enhancing the cybersecurity of medical devices. CHIME and AEHIS welcome the opportunity to offer our members perspective and we appreciate your attention to this important issue. Should you have any questions or if we can be of assistance to the Committee, please contact CHIME's Vice President of Congressional Affairs, Leslie Krigstein at lkrigstein@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME

Will Long
Chair, AEHIS Advisory Board
Vice President & CISO
Children's Health