June 1, 2018

The Honorable Rodney Frelinghuysen
Chairman
House Committee on Appropriations
H-305, The Capitol
Washington, DC 20515

The Honorable Nita Lowey
Ranking Member
House Committee on Appropriations
1016 Longworth House Office Building
Washington, DC 20515

The Honorable Robert Aderholt
Chairman
House Subcommittee on Agriculture, Rural Development, Food and Drug Administration and Related Agencies
2362-A Rayburn House Office Building
Washington, DC 20515

The Honorable Sanford Bishop
Ranking Member
House Subcommittee on Agriculture, Rural Development, Food and Drug Administration and Related Agencies
1016 Longworth House Office Building
Washington DC, 20515

Re: Fiscal Year 2019 House Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Report -- Cybersecurity in Medical Devices

Dear Chairman Frelinghuysen, Ranking Member Lowey, Chairman Aderholt and Ranking Member Bishop,

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) enthusiastically support the language included in the Fiscal Year 2019 House Agriculture, Rural Development, Food and Drug Administration and Related Agencies Appropriations Report directing the Food and Drug Administration (FDA) to examine cybersecurity in medical devices. We appreciate the Committee's interest in ensuring lifesaving medical devices are secured and welcome the opportunity to offer perspective from the nation's healthcare chief information officers (CIOs) and chief information security officers (CISOs).

CHIME is an executive organization that serves more than 2,600 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 800 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. Just in healthcare alone, the growth of IoT connections from 2014 to 2015 increased by 26 percent.[1] Tens of thousands of medical devices can be used throughout large healthcare systems, many of which are connected directly to the patient or

[1] *State of the Market: Internet of Things 2016, https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf*

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.

With cyberattacks like Petya and WannaCry showing just how vulnerable some network connected devices can be, action must be taken to secure the healthcare sector. 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.

CHIME and AEHIS members applaud the below language included in the FY19 Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Committee Report.[2]

> *"Cybersecurity in Medical Devices.—The Committee believes that the FDA should address potential cybersecurity vulnerabilities in medical devices in general, but especially as the Internet of Things becomes more prevalent in healthcare. The Committee directs the FDA to report back within 120 days on the agency's plans to understand the ongoing cybersecurity challenges of medical devices and outline a pathway forward. The plan should describe potential solutions and list compensating controls such as continuous inventory, log monitoring, data protection, micro segmentation, and patching on legacy devices to prevent cyber threats from spreading across hospital systems. The Committee encourages the FDA to seek industry collaboration to uncover the extent of the vulnerabilities and threats with a representative pathway to solving this critical issue."*

The requested FDA report 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 us at policy@chimecentral.org.

Sincerely,

Cletis Earle, Chair
CHIME Board of Trustees Vice President,
CIO Information Technology
Kaleida Health

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

cc: The Honorable Richard Shelby, Chairman, Senate Committee on Appropriations
The Honorable Patrick Leahy, Ranking Member, Senate Committee on Appropriations
The Honorable John Hoeven, Chairman, Subcommittee on Agriculture, Rural Development, Food and Drug Administration, and Related Agencies, Senate Committee on Appropriations
The Honorable Jeff Merkley, Ranking Member, Subcommittee on Agriculture, Rural Development, Food and Drug Administration, and Related Agencies, Senate Committee on Appropriations

[2] https://docs.house.gov/meetings/AP/AP00/20180516/108312/HRPT-115-HR-FY2019-Agriculture.pdf