March 18, 2019

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

Re: *Content of Premarket Submissions for Management of Cybersecurity in 2 Medical Devices*

Dear Commissioner Gottlieb:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to submit comments on the Food and Drug Administration's (FDA) draft guidance published October 18, 2018, the *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*. We strongly support the several policy proposals and plans the agency is advancing, including the policies contained within this draft guidance, which take into account the serious threats to patient safety stemming from cybersecurity threats to medical devices.

CHIME is an executive organization dedicated to serving chief information officers (CIOs) 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 850 chief information security officers (CISOs) and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topic of cybersecurity and they take their responsibility to protect the privacy and security of patient data and devices networked to their system very seriously.

Appended to this letter you will find our detailed recommendations concerning suggested edits to the draft guidance. Below, however, is a summary of our top recommendations and feedback.

1. **Devices are part of an ecosystem:** An infected device can serve as a beachhead for intruders intent of gaining entry to a healthcare provider's network. Since devices are part of a larger healthcare technology ecosystem, it is important to recognize that patient safety threats being discussed extend well beyond medical devices, even if they originate there. Therefore, singling out medical devices without recognizing that there are networks, switches, firewalls, applications and other components that come with medical devices does not adequately capture the risks. For instance, an infusion pump needs to connect to a controlling application, a drug library, etc. for it to function. And, if the pump becomes infected with malware, it may need to be removed from a hospital network. As such, the patient safety implications stem well beyond the device itself. While a provider can remove a device from their network and thus sever the ability of the attack to

further perpetrate their system, there can be downstream patient safety implications from removing the connected device since the device functionality might be limited in its ability to treat the patient.

Recommendation: FDA should add to their definitions list (starting line 192) one for "medical devices." The definition should recognize that medical devices are part of an overall ecosystem which includes but is not limited to networks, switches, firewalls, applications and other components that come with 'medical devices'.

2. **Manufacturer perceptions of guidelines:** We appreciate that the FDA is attempting to maintain a flexible regulatory environment by publishing "guidelines" as opposed to rulemaking. That said, many of our members continue to be confronted with some manufacturers who refuse to take action on known vulnerabilities choosing either to categorize them as "controlled risks" or saying they will wait until the FDA recalls a device. For example, many of our members still report that patch MS17-010 (the patch that protects against WannaCry) has still not been deployed to certain medical devices due to the manufacturers classifying that vulnerability as a Controlled Risk. This is nearly 2 years after the national response to WannaCry, Petya and NotPetya. From our perspective both of these scenarios are unacceptable. Importantly, we believe that the FDA must be as explicit as possible with manufacturers around their expectations. Without clear direction to the manufacturers about what is required, the burden of proof for demonstrating a standard has been met and devices are secure will be shouldered by providers.

   Recommendations: The agency should make more explicit the steps a manufacturer must meet to first and foremost ensure patient safety is protected; and second to inoculate providers from taking on undue risk which ultimately can cascade into patient safety risks.

   The FDA should also consider requiring device manufacturers meet a certification standard. This is already commonplace for electronic health records (EHRs) and there is far more transparency around what these vendors must meet.

3. **Legacy devices:** Most health systems have tens of thousands of legacy devices in their systems. KLAS research has found that the top manufacturer-related factors causing medical device security issues.
   The Health Care Industry Cybersecurity Task Force report from 2017 also had this to say, "Legacy systems include both legacy medical devices and legacy EHR applications, which may not have any ongoing support from the hardware and software vendor(s) that provided these solutions. They may impact the entire system or system components, including firmware, drivers, operating systems, and all applications in use. Many of these legacy systems have security weaknesses, which may contribute to the compromise of provider networks and systems. Every vendor and health care organization should be able to identify and classify legacy systems and develop an

approach (e.g., compensating controls, device update, device retirement, network segmentation, or innovative architectures) to mitigate the associated risks." Given the well-chronicled challenges providers face with legacy devices, both providers and manufacturers need help securing medical devices.

> **Recommendations: The FDA's pre-market guidance should explicitly reference the voluntary guidance co-developed by industry in conjunction with the U.S. Department of Health & Human Services (HHS) intended to serve as resources and tools to aid both parties improve their cybersecurity posture. Specifically, the FDA should reference the Medical Device and Health IT Joint Security Plan and the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.**
>
> **Furthermore, the FDA should also reference NEMA CPSP 1-2015 - Document ID: 100742 (Supply Chain Best Practices), NEMA CPSP 2-2018 - Document ID: 100828 (Cyber Hygiene Best Practices), and HIMSS/NEMA HN 1-2013 - Document ID: 100382 (MDS2).**

4. **Obsolete operating systems:** Many devices contained antiquated operating systems which are no longer being updated by the developer. Our members have estimated that as many as 35%-45% of devices within health systems are end of life – possibly even higher in rural settings. The FDA recognizes the risks for end of life devices when patches or updates are no longer available. However, software should be considered part of the device and thus embedded software should be more explicitly addressed.

   > **Recommendation: Software should be included in the discussion of a device's "essential performance" (line 124). Additionally, we recommend under the requirements for authenticating and checking authorization of safety-critical commands that user authentication be required before permitting software or firmware updates, including those affecting the operating system, applications, and security controls (lines 411-413).**

5. **Patient Safety:** We do not believe the definition of patient safety and harm are synonymous. Patient safety signifies all the risk leading up to where a patient can be harmed. Additionally, from an ecosystem standpoint patient safety may not represent a single patient, rather, it can signify the general principle of patient safety as a whole.

   Separate, but related to the topic of patient safety, are privacy issues. We continue to assert that the privacy issues, while the domain of Office for Civil Rights (OCR), still has a place in FDA guidance [as previously articulated in our April 21, 2016 letter to the FDA in our comments on the draft, "Postmarket Management of Cybersecurity in Medical Devices" (Docket No. FDA–2015–D–5105, published January 22, 2016] and that more attention on privacy issues – not just security – is warranted. Further, we disagree with the notion that developers should be the ones to

unilaterally decide whether a risk is controlled or uncontrolled. We do not believe this type of self-policing is fruitful. In fact, providers are held to a much higher standard under OCR privacy rules around breaches and must prove protected health information has not been compromised in the case of a breach.

Recommendations: The FDA should add a new definition for patient safety (to line 202), in addition to the definition for patient harm (line 199).

Additionally, the FDA should work collaboratively with the OCR to communicate to the public and various impacted stakeholders that cybersecurity is a shared risk. The FDA should issue two sub-categories under both "controlled" and "uncontrolled" risks. The first sub-category should be aimed at patient safety and the second aimed at information risks (in particular, though not limited to, privacy issues). FDA should work collaboratively with OCR to share information risks that are related to patient privacy.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Sean Murphy VP & CI
Premera
Chair, AEHIS