August 22, 2018

Seema Verma
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Administrator Verma:

The Association for Executives in Healthcare Information Security (AEHIS), an affiliate organization of the College of Healthcare Information Management Executives (CHIME), is pleased to submit comments to the Centers for Medicare and Medicaid Services' (CMS) proposed rule, "Medicare Program; Request for Information Regarding the Physician Self-Referral Law," published in the *Federal Register* on June 25.

Launched by CHIME in 2014, AEHIS represents more than 900 chief information security officers and provides education and networking for senior IT security leaders in healthcare. Please find our ideas for a safe harbor pertaining to donations involving cybersecurity outlined below. As CMS is aware, the healthcare industry is an interconnected ecosystem whereby the 'weakest link' in the chain of trust can be the point of compromise for the whole system.

AEHIS believes one way the threat environment in healthcare can be made more secure is to help providers who are lesser resourced and who would benefit from services that will help strengthen their cybersecurity posture. In particular, we are interested in seeing CMS permit donations of cyber services and technologies. We request that you review the following statistics as you consider this request:

- Our healthcare industry is at "great risk of a cyberattack that could seriously impact the safety of patients," concludes the Health Care Industry Cybersecurity Task Force.[1]
- The healthcare sector is among a handful of sectors that have experienced the highest number of breaches.[2]
- One in 131 emails have malware, a five-year high.[3]
- 43% of organizations surveyed by KLAS[4] have not developed or are in the process of developing a cybersecurity program.

[1] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
[2] https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[3] https://www.symantec.com/security-center/threat-report
[4] KLAS, "Cybersecurity 2017 Understanding the Healthcare Security Landscape, "February 2017 Performance Report, https://klasresearch.com/report/cybersecurity-2017/1121.

- There has been a 320% uptick in the number of healthcare providers who were the victims of a cyberattack.[5]

A priority for AEHIS is to advance policies that facilitate better cybersecurity posture among our members and others with whom they do business. Our efforts are intended to fortify the healthcare infrastructure, which has long been identified as one of the 16 critical infrastructures. As such, we are looking for ways to help incent better cybersecurity hygiene among healthcare providers who often face limited resources and competing priorities. Strengthening the health and public health infrastructure – if for no other reason – will better safeguard patient safety. Patient care and safety are being jeopardized daily by a barrage of cybersecurity attacks, including those that pose a threat to medical devices. Added to this are additional threats to this sector which have moved from a trickle to a flow with the Internet of Things. This interconnected environment poses additional risks as other, non-medical devices, are increasingly being connected to a health system's ecosystem (i.e., smart microwaves and heating, ventilation, and air conditioning (HVAC) units). Given these factors, the healthcare sector has become prime target for cyberattacks.

In addition to these alarming statistics, the Cybersecurity Industry Task Force Report which was mandated by the Cybersecurity Act of 2015, includes an entire section (page 35) that discusses the myriad of issues associated with the anti-kickback and Stark statutes. The report says:

> *A regulatory exception to the Stark Law and a safe harbor to the Anti-Kickback Statute to protect certain donations of electronic health records (EHR) effectively addresses management of technology between health care entities and serves as a perfect template for an analogous cybersecurity provision. Physician groups confront a myriad of financial challenges. Often these financial constraints limit their ability to manage the EHR software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower small providers or suppliers (e.g., physician practices) to actively manage their security posture, not hinder them. Often organizations want to provide technology to ensure smaller business partners do not become a liability in the supply chain. An exception may provide for this assistance without creating fear of violating the Stark Law or Anti-Kickback Statute.*

Given the foregoing concerns, the recommendations from the Task Force report, and the need identified by many of our members, we strongly believe an exemption to the Stark statute that permits for donations of services that further an entity's cybersecurity posture is warranted. We recognize there may be limitations around how such an exemption is crafted; however, if it followed many of the requirements that the CMS laid out around the exceptions permitted for donating an electronic health record (EHR), this would be helpful. **Ideally, we recommend that the CMS tailor an exemption that permits donations of training / education services, software and technology. Technologies with the greatest impact on improving cybersecurity hygiene, as identified by CIOs and CISOs, include: firewalls / intrusion**

[5] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

detection and prevention systems, antivirus / malware, email filtering / encryption, data loss prevention software, and advisory services.[6]

We appreciate the opportunity to comment and we welcome the opportunity to discuss these issues in more depth with CMS. Please contact Mari Savickis, vice president, federal affairs, at mari.savickis@chimecentral.org to help facilitate a meeting and continue the dialogue.

Sincerely,

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

[6] KLAS, "Cybersecurity 2017 Understanding the Healthcare Security Landscape, "February 2017 Performance Report, https://klasresearch.com/report/cybersecurity-2017/1121.