February 26, 2018

Daniel Levinson
Inspector General
Office of Inspector General
Department of Health and Human Services
ATTN: OIG-127-N
330 Independence Avenue, SW
Washington, DC 20201

Dear Inspector Levinson:

The Association for Executives in Healthcare Information Security (AEHIS), a sister organization under the College of Healthcare Information Management Executives (CHIME), is pleased to submit comments to the Office of Inspector General (OIG) regarding *Solicitation of New Safe Harbors and Special Fraud Alerts*, published December 27. Launched by CHIME in 2014, AEHIS represents more than 800 chief information security officers and provides education and networking for senior IT security leaders in healthcare. Below, please find our ideas for a safe harbor pertaining to donations involving cybersecurity.

A priority for both organizations is to advance policies that facilitate better cyber posture among our members and others with whom they do business. Our efforts are intended to fortify the healthcare infrastructure which continues to lag the other 15 critical infrastructures. As such, we are looking for ways to help incent better 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 is being jeopardized daily by a barrage of cyber attacks that pose a threat to medical devices. Adding 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 HVAC units). Together, the healthcare sector has become a prime target for cyberattacks.

CHIME and AEHIS believe 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 cyber posture. In particular, we are interested in seeing the OIG permit for donations of cyber services and technologies. We request that you review the following sobering statistics as you consider this request:

- Our healthcare industry is at “great risk of a cyber-attack 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 who 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 security program
- There has been a 320% uptick in the number of healthcare providers who were the victims of a cyber hack.[5]

In addition to these alarming statistics, the Cybersecurity Industry Task Force Report[6] which was mandated by the Cybersecurity Information Sharing Act of 2015 (CISA), includes an entire section within their report (page 35) which 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 anti-kickback statute that permits for donations of services that further an entity’s cyber 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 OIG laid out around the exceptions permitted for donating an electronic health record (EHR), this would be helpful. **Ideally though, we recommend that the OIG tailor an exemption that permits donations of training / education services, software, and technology. Technologies with the greatest impact on improving**

[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.

[5] https://insights.cynergistek.com/reports/2016-breach-report

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

cyber hygiene, as identified by CIOs and CISOs include firewalls / IDPs, antivirus / malware, email filtering / encryption, DLP, and advisory services.[7]

We welcome the opportunity to discuss these issues in more depth with the OIG and would be pleased to facilitate a meeting to discuss these ideas. Mari Savickis, vice president, federal affairs, at msavickis@chimecentral.org can help facilitate such a meeting.

Sincerely,

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

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