CHIME
College of Healthcare
Information Management Executives

October 26, 2018

Daniel R. Levinson
Inspector General
30 Independence Avenue, SW,
Washington, DC 20201

Dear Inspector Levinson:

The College of Healthcare Information Management Executives (CHIME) welcomes the opportunity to submit comments regarding the "Medicare and State Health Care Programs: Fraud and Abuse; Request for Information Regarding the Anti-Kickback Statute and Beneficiary Inducements CMP," published in the *Federal Register* on August 27th.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With more than 2,800 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of technology to improve the health and healthcare in the communities they serve.

We appreciate the Administration's efforts to reduce regulatory burdens on healthcare providers, including reviewing how changes to the anti-kickback rules could foster an easier pathway to value.

High-level Feedback

1. **Cybersecurity threats pose a risk to patient safety;**
2. **We support a stand-alone cybersecurity safe harbor that permits the donation of related items and services; and**
3. **OIG anti-kickback requirements and safe harbors should be aligned with Federal Trade Commission (FTC) requirements for clinically integrated networks (CINs).**

Cybersecurity-Related Items and Services

CHIME appreciates OIG has listened to our previous feedback on the importance of cybersecurity. Moreover, we are pleased that the OIG is considering the recommendation made in the Health Care Industry Cybersecurity Task Force report, which calls for examining "potential impacts to the Physician Self-Referral Law, the Anti-Kickback Statute, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners."

The RFI indicates OIG is exploring additional ideas for how an arrangement could be structured to permit the donation of cybersecurity-related items and services. We strongly support establishing a safe harbor that permits entities to donate these types of items and services, particularly to both under-resourced providers, as well as providers who need help fortifying their cybersecurity posture. We are furthermore pleased with recent announcements by the Food and Drug Administration (FDA) prioritizing cybersecurity and patient safety. Importantly, our members firmly believe that cybersecurity is a threat to patient safety and it is a national imperative and shared responsibility that we work together to strengthen our industry's posture, which to date has lagged other critical infrastructures. In fact, in a recent report we co-authored with KLAS, providers cited their significant concerns with patient safety as among their top issues with medical devices. Many of the devices are delivered "off the pallet" to providers with known (and unknown vulnerabilities) making the challenge of protecting patients and the costs for doing so even greater. And, some of our members continue to report: 1) some device manufacturers still refuse to patch vulnerabilities (i.e. some members still have not received patches following the WannaCry attack launched more than a year ago); and 2) they still struggle with getting favorable contract language from manufacturers and vendors that protects their cyber posture; lesser-resourced providers face even greater challenges.

Many providers, especially smaller ones, have taken advantage of the option to accept donated electronic health records (EHRs) as a result of the safe harbor permitting this. A likeminded safe harbor for cybersecurity would thus be welcomed by some of our members. While many of our members have said they worry about taking advantage of cybersecurity donation safe harbor for fear that if they donated these types of items and services and a recipient experienced a cyberattack, that this could expose them to risk. However, other members felt the risk would be managed through contracts and by way of securing their own network. Some of our members they felt a waiver would allow them to aid smaller, affiliated hospitals in their area; and since they are all connected to the same networks, helping the lesser resourced entities would be helping everyone. So much of our health system is increasingly integrated that providers with weaker cyber postures can pose threats to other providers. Therefore, permitting donations to those providers who need more help, from our perspective, makes sense. While some have discussed the notion of modifying the existing EHR safe harbor, we recommend a separate, stand-alone safe harbor specifically designed for the purposes of supporting the donation of cybersecurity items and services.

Additionally, in considering how to structure a cybersecurity donation safe harbor, we recommend OIG take into account the following points:

- Requiring a receiving provider to have some investment in the donation, as is the case with the EHR safe harbor, is reasonable.
- The cost of the items and services need to be affordable for lesser resourced providers. For instance, many are unable to afford hiring a security architect, engineer, or chief information security officer, or a consulting firm. Donations, therefore, become a workable option.
- The types of items and services we envision could be included in an allowable donation include (but are not limited to):
    - Security program development
    - Helping perform risk assessment (the most failed area under the Meaningful Use / Promoting Interoperability program)
    - Software (i.e. licenses) which allows for patching
    - Hardware
    - Expertise following a cyberattack
    - Staff time / human capital resources (i.e., a large integrated delivery system might serve as a security operations center (SOC))

Finally, given the volume of data being exchanged in healthcare, the rapid proliferation of the Internet of Things, the widespread uptake of EHRs, and that the average number of connected devices across providers of various sizes is 10,000, it is imperative that we do everything possible to fend off millions of cybersecurity threats launched at providers daily. A real-time threat map demonstrating where the threats are originating (i.e. Russia and China) can be found here.

Clinically Integrated Networks

We are pleased the Administration's regulatory sprint is aimed at identifying policies that hinder the transition to value. The OIG has requested feedback on potential arrangements that the industry is interested in pursuing, such as care coordination, value-based arrangements, alternative payment models, arrangements involving innovative technology, and other novel financial arrangements that may implicate the anti-kickback statute or beneficiary inducements CMP.

Most of our members participate in provider partnerships for value-based contracting including Accountable Care Organizations and Clinically Integrated Networks currently governed under FTC anti-trust rules. FTC allows ACOs and Clinically Integrated Networks to collaborate with otherwise independent healthcare providers to improve quality and contain costs. As outlined in our comments in response to CMS' RFI on Stark, providers participating in these partnerships are already subject to a number of FTC requirements. In reviewing the OIG's RFI, while we are pleased to see the agency considering safe harbors around several areas including innovative uses of technology, we did not see any mention of the FTC requirements. Our members who are complying with the FTC requirements have already done much of the work to support the Anti-Kickback Statute and would like to understand how the current framework allows or needs to be enhanced to provide increased value-based care services with different continuum providers (i.e., home technology support services), provide beneficiary support for family care givers and/or allow for beneficiary incentives for health goal achievements that increase quality and decrease cost. Thus, those providers participating in the FTC partnerships currently have done the leg work needed to support the services OIG is considering allowing. **We recommend OIG align AKS requirements and safe harbors with what is required by the FTC partnerships.**

Conclusion

CHIME appreciates the opportunity to comment and welcomes the chance to discuss our comments with OIG in greater depth. Should you have questions about our letter please contact Mari Savickis, vice president of federal affairs, at mari.savickis@chimecentral.org.

Sincerely,

Russell P. Branzell

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

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