

December 31, 2019

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

Acting Inspector General Joanne Chiedi  
Office of Inspector General  
U.S. Department of Health and Human  
Services  
Cohen Building  
330 Independence Avenue SW,  
Washington, DC 20201

Dear Administrator Verma & Acting Inspector General Chiedi:

The Healthcare and Public Health Sector Coordinating Council (HSCC) is pleased to comment on the *Medicare and State Healthcare Programs: Fraud and Abuse; Revisions To Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements* published by the Office of Inspector General (OIG) and the *Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations (CMS-1720-P)* published by the Centers for Medicare & Medicaid Services (CMS), companion proposed rules both published on October 17, 2019 in the *Federal Register*.

The HSCC is a private sector-led advisory council of major health industry stakeholders working together and with the U.S Department of Health & Human Services (HHS) to identify and mitigate threats and vulnerabilities affecting the ability of the sector to deliver healthcare services to the nation's citizens. A major component of the HSCC is its Cybersecurity Working Group, which represents 215 healthcare organizations in the subsectors of direct patient care, medical materials, health information technology, health plans and payers, laboratories, biologics and pharmaceuticals, and public health. Our members collaborate toward improving the cyber security and resiliency of the healthcare industry and patient safety.

The diverse organizations representing the HSCC have a vested interest in advancing the cyber posture of the healthcare industry and improving patient safety. Our members are responsible in different capacities for protecting and securing patient information - a fundamental imperative to supporting a healthcare system that is driven by value rather than volume.

These comments will focus on the cybersecurity proposals of the companion rules.

**We are grateful for the proposals that align with recommendations we and several other stakeholders made concerning establishing an exception / safe harbor for the donation of cybersecurity technology and services. We applaud this move and believe it will lend much-needed support to providers who are already grappling with cybersecurity threats that are growing both in volume and complexity.**

The Healthcare Industry Cybersecurity Task Force Report<sup>1</sup>, which was mandated by the Cybersecurity Information Sharing Act of 2015 (CISA), includes more than a hundred

---

<sup>1</sup> <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>

recommendations for how the healthcare sector can improve its cyber posture. The report includes a discussion (page 35) on the various 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.*

In developing their proposal for a cyber exception / safe harbor, the agencies pointed to the recommendation made by the Task Force. We appreciate that the Administration is promulgating this recommendation through rulemaking.

Based upon our review of the cybersecurity exception / safe harbor proposal laid out by CMS and OIG we have four overarching topics for consideration.

1. **Small and under-resourced providers:** We appreciate that CMS and OIG are concerned with small and under-resourced providers' ability to invest in technology and services to protect their infrastructure and safeguard patient data. We support policies that will aid these providers, as the healthcare ecosystem is increasingly interconnected. The better small and under-resourced providers can protect themselves, the better it is for the entire system. Cyber vulnerabilities, as we have seen, can spread very quickly and it is imperative these providers are assisted in what has become an unduly difficult task, even for the best resourced providers. Further, the proposed exception / safe harbor will support the exchange of information and interoperability.
2. **Patching:** Providers have an on-going obligation to protect their technology and safely provide patient care. In many cases, the technology (or accompanying security updates/fixes) would not be a one-time donation but something that would need to be maintained over time in the case of hardware and software. Patching and updates are widely accepted as being critical to guarding against cybersecurity threats. In fact, in materials jointly developed by the U.S. Department of Health & Human Services (HHS) and the industry as part of the CISA 405(d) Task Group call out the lack of patching as a significant vulnerability and recommend it as a best practice.<sup>2</sup> Further, information technology systems are not static, but living systems that require constant changes. Both CMS and OIG have proposed that patching and updates will not be an allowable donation that would receive protection under the exception / safe harbor. Feedback we received from members suggested this could create significant complications in disaggregating when technology is permitted to be donated. Often, patching is given to providers for free as it is built into the contracts with vendors. We request clarification on

---


<sup>2</sup> <https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>

whether accepting a routine or critical updates would implicate a violation of the exception / safe harbor. Some patches also may be aimed at security while others may be more general. Have CMS and OIG considered permitting patching when it is needed for security purposes?

3. **Definition of Technology:** Both CMS and OIG have called for excluding hardware from the permitted type of technology which is protected under the cybersecurity donation exception / safe harbor. We are concerned this approach could impede the success of this exception / safe harbor. First, the lines between what is considered hardware vs software is increasingly being blurred. Also, by breaking out hardware from the definition of technology it does not account for the pace of innovation. Second, vendors do not typically break out the cost of hardware vs software – the price or value is based upon the totality of the device. An example would be a networking device that is running software. Precluding the donation of hardware, therefore, could create barriers to donations of cybersecurity technology if donors and recipients aren't clear how to disaggregate the two.
4. **Written Agreement:** We concur with the proposal by CMS and OIG that a written agreement between the donor(s) and recipient will bring transparency to the donation process.
5. **Voluntary:** CMS and OIG have made clear that the cybersecurity donation exception and safe harbors are voluntary, meaning, there are no requirements that providers must donate to other (i.e. small) providers' cybersecurity technology or services. We support this proposal and agree that donations should not be mandatory. Some providers have raised concerns about liability. Clarification from CMS and OIG on whether providers will be offered some safe harbor if a recipient of donated technology experience a cyber-attack, would be helpful.
6. **Liability:** One issue that has been raised by some providers is around the issue of liability. Several providers have expressed concern that donor providers could incur significant liability if the recipient of donated technology experiences a cyber incident. Additionally, if a donating entity does a risk assessment of a physician's practice and misses something or the practice suffers an attack, what kind of liability will the donor incur? Without some sort of protection for the donating provider, some providers are unlikely to take advantage of this donation exception / safe harbor.

The HSCC CWG appreciates the opportunity to comment on this proposal and for CMS and OIG making cybersecurity a priority.

Sincerely,



Greg Garcia, Executive Director

HSCC Cybersecurity Working Group