HIMSS Electronic Health Record Association

33 W Monroe, Suite 1700
Chicago, IL 60603
swillis@ehra.org
Phone: 312-915-9518
Twitter: @EHRAssociation

December 20, 2019

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

Joanne Chiedi
Acting 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:

Thank you for the opportunity to comment on the companion proposed rules: *Medicare and State Healthcare Programs: Fraud and Abuse; Revisions To Safe Harbors Under the Anti-Kickback Statute (AKS Proposed Rule), 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 (Stark)* published by the Centers for Medicare & Medicaid Services (CMS), both published in the Federal Register on October 17, 2019.

The 32 members of the Electronic Health Record Association serve the vast majority of hospitals and ambulatory care organizations that use electronic health records (EHRs) and other health information and technology to deliver high quality, efficient care to their patients. Our core objectives focus on collaborative efforts to accelerate health IT adoption, advance interoperability, and improve the quality and efficiency of care through the use of these important technologies.

The EHR Association is pleased to see CMS and OIG continue efforts to support widespread adoption of robust health IT technologies that can support providers in delivering optimized care and exchanging clinically relevant health information.

The Stark and Anti-Kickback rules have had a significant impact on EHR adoption for many years, and we support most of the proposals that have been released to update these regulations.

The adjustments that have been proposed would allow organizations that have been slow to digitize to consider this model for funding, and also provide for practices with older EHRs to replace them with newer technologies. That is a positive change.

We appreciate the effort to more closely associate the Stark and Anti-kickback safe harbors with care coordination gaps in healthcare. Coordinating care across multiple, lightly affiliated entities requires thoughtful governance and policies as well as skillful navigation, and no single model is proven for success. Therefore, EHR Association members suggest that CMS and OIG invest resources against the challenge of repeatedly educating the provider community in this area.

EHR Association members recognize that the concepts related to consumer engagement and the role that devices play in the patient's care and outcomes could be found to be insufficient in the proposed rules from CMS or OIG. We do support the creation of a new safe harbor "for certain tools and support furnished under patient engagement and support arrangements to improve quality, health outcomes, and efficiency" (1001.952(hh)). Giving patients a device to communicate with a care team should not be considered a beneficiary inducement, and software-based platforms for patient-generated health data or telemedicine should be allowable under Anti-kickback rules, as it is clear that such tools are the future of tracking and sharing data. Also, we suggest that with the availability of rapidly evolving technologies, tools, and programs to engage consumers that the final rules should recognize such development and not unnecessarily preclude them from consideration for safe harbors, e.g.,applications on a phone, such as a diabetes management app or an annual membership in a weight loss tracking app.

The Association's detailed comments follow:

II.A. Facilitating the Transition to Value-Based Care and Fostering Care Coordination

The Association applauds CMS and OIG for the proposals that will enable more physicians to take part in value-based care. Continuing to expand regulatory relationships between value-based behaviors and payments, reimbursements, or other financial incentives will serve to support efforts to transform overall healthcare delivery system by focusing on patient-centered care, innovation, and outcomes.

While the self-referral rules are important to prevent providers from increasing their revenue based upon where a patient is referred; under these proposals, there is potential benefit for patients to receive more comprehensive care. We do have continued concerns about the limited opportunities for smaller, independent physician practices to participate in value-based payment models, and the limitations proposed here would seem to exacerbate that problem. We are aware that CMS has rolled out programs in the past year intended to increase small practice options, yet there is still a very large portion of that population in regions without option. Or, some of the proposed programs aimed at small

practices are incompatible with their practice structure (direct primary care practices, for example), too burdensome in the requirements, or unsupported by their health IT supplier because the program's technical requirements surpass those of ONC certification. We strongly encourage CMS to revisit existing programs and rapidly consider others that would help small practices to join a value-based payment program and thus become eligible for this Stark funding model. Otherwise, practices may see this as yet another reason that they can no longer maintain independence, an issue HHS has identified previously as an area of concern.

Also, EHR Association members observed that in some cases the definitions in the proposed rule are broad and vague, leaving room for interpretation. CMS and OIG should use more specific language where possible and provide examples of services that would be allowed under these exceptions. For example, the final rules should be clear that durable medical equipment may be included if, and only if, those costs are included in the global payment. Moreover, in the definition, we recommend that fee-for-service components of a new payment model still be subject to self-referral statutes and that regulators clearly outline this in the final rule.

Finally, regarding this section, the Association requests that CMS and OIG clarify references to "reducing costs" and addresses such questions as, cost to whom? The payer? The patient?

II.D.11. 11. Electronic Health Records Items and Services (§411.357(w))

EHR Association members thank CMS and OIG for proposing to update the language associated with electronic health records and services to align it with the language in the 21st Century Cures Act. As expressed previously on a number of occasions, EHR developers are challenged when definitions or requirements do not align across programs.

We understand the current Deeming Provision specifies that software is deemed to be interoperable if, on the date it is provided to the physician, it has been certified by a certifying body to an edition of the electronic health record certification identified in the then-applicable version of 45 CFR part 170. Regarding the proposal to remove the reference to "an edition," we agree with this proposal and recommend that the language read "latest or current" edition or wording to a similar effect.

II.E.2. Cybersecurity Technology and Related Services (Proposed §411.357(bb))

The EHR Association applauds CMS' effort to open additional avenues to combat cybersecurity threats. We and our collective clients live every day with the challenge of thwarting attempts at inappropriate access and data exfiltration. Our success will depend on partnerships between private and public stakeholders.

First, we recommend that if this proposal is finalized, integrated hardware (such as tokens, key fobs, and cameras used for facial recognition) be permitted for multi-factor authentication purposes. The distinction between software and hardware is not as straight-forward as it was when the Stark and AKS safe harbors were first conceived, and we suggest that more flexibility be allowed.

There are factors related to cybersecurity that are different than the other types of denotable software and services that have traditionally been addressed by CMS and OIG. Given the fast-paced nature of cybersecurity, it is likely that new tools will need to be deployed on an annual basis (or even more often). Any final rule on this topic should address this difference from the software and services more traditionally donated.

We noticed that the proposed rule does not address a fundamental element of any cybersecurity strategy: people. Thus, we are concerned that organizations receiving an allowable cybersecurity donation may have a false sense of confidence; it has the potential to give the impression that responsibility for cybersecurity has shifted from the practice to the donor.

In reality, however, cybersecurity is more than just technology tools; it is about human behavior, which is difficult to control (e.g. when someone unknowingly clicks on a malicious link in a phishing email). The healthcare ecosystem needs significant education and training, especially because tools in this space are required, by their nature, to be ever-changing and evolving to keep up with new threats. We strongly encourage CMS and OCR to dramatically increase educational opportunities in this area. Also, we recommend that the Regional Extension Centers increase the work they do with small practices to train on cybersecurity workflow best practices. This would have the added benefit of avoiding an uneven/unbalanced relationship between smaller practices and the donor, such that practices are relying on the donor for software but less so for overall cybersecurity strategy.

Additionally, the EHR Association remarks that the industry as a whole remains largely ignorant of the factors that played into successful cybersecurity attacks experienced so far by various players across the sector. In order to improve behavioral compliance, we recommend that CMS partner with ONC and OCR to study the root cause of past ransomware attacks and leverage the results to influence policy recommendations and craft educational programs for healthcare organizations.

Finally, we urge CMS to consider these proposals in the context of public cloud offerings. With some pricing models, cybersecurity tools are bundled into a fixed cost for the larger technology system. CMS should consider how the proposal will work with tracking and maintaining a fair, reportable anti-kickback funding system.

III.I.3 Information Blocking (Proposed 1001.952(y)(3))

OIG has attempted to create a tie-in between the AKS proposed rule and the ongoing efforts to implement the Information Blocking provisions of the 21st Century Cures Act ("Cures"). Accordingly, there is a limitation proposed to the definition of value-based activity as it relates to information blocking. Specifically, the proposed rule states:

> *"preclude from protection under our proposed safe harbors at 42 CFR 100.952(ee), (ff) and (gg) any arrangement that may, on its face, meet our definition of value based activity but that ultimately is used to engage in practices of information blocking (e.g., the donation of health information*

technology that may facilitate care coordination across providers participating the VBE, but also prevents or that unreasonably interferes with the exchange of electronic health information with other providers in order to lock-in referrals between such providers). Information blocking practices that may affect value-based activities include, but are not limited to, (1) locking electronic health information into the VBE or keeping it only between VBE participations or (2) preventing referrals or other electronic health information from leaving the VBE or being transmitted from a VBE participant to another health care provider."

As an Association, we support all efforts to diminish and ultimately end any activities aimed at blocking information. As proposed in the Cures regulation, we expect that information blocking prohibitions will be wide-ranging and apply to stakeholders across the industry, including but not limited to those subject to the Anti-kickback statute. Furthermore, because of the many questions raised around how information blocking will be investigated and adjudicated, we anticipate the adoption of additional processes and guidance surrounding implementation and enforcement.

On the other hand, the application of the expected information blocking regulation to the statute introduces an additional layer of ambiguity to the exception. The federal Anti-kickback statute is an intent-based, criminal statute and already has protections that prevent misuse of the safe harbors. Because this type of regulation is limited in effectiveness, if there is any noteworthy ambiguity, as we noted in previous comments and letters responding to the ONC NPRM on Interoperability and Information Blocking, we suggest that either OIG provide additional examples related to its application in the final rule, or that OIG, CMS, and ONC coordinate closely on the intersection between information-blocking enforcement and the Anti-kickback safe harbors.

In particular, there exists the risk that a small practice and a large hospital may enter into an arrangement made possible through these safe harbors, but a future determination of information blocking against either of those entities undermines the stability of that allowable financial relationship. This could leave the small practice vulnerable to unexpected costs or even lost access to its health information technology if the hospital no longer pays for it, requiring the small practice to quickly establish its own EHR/health IT infrastructure and potentially putting patients at risk during any extended system down-time. We suggest that a curative period be allowed within any such situation so that behavior determined to be information blocking may be resolved before the recipient has to stop using the EHR, or otherwise enable the small practice to establish its own infrastructure.

Alternatively, because the information blocking provision is already anticipated to go far beyond participants who might be affected by the Stark and Anti-kickback statutes, OIG and CMS could simply assume that information blocking will no longer be tolerated regardless of any sort of value-based care arrangement and leave the enforcement of information blocking restrictions to the regulation finalized in 45 CFR §171.

Thank you for this opportunity to provide our perspective and expertise in your combined efforts to support widespread adoption of robust health IT technologies that can support providers in delivering optimized care and exchanging clinically relevant health information. If the EHR Association can be of further assistance, please contact Jessie Bird at jbird@himss.org.

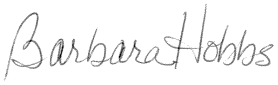
Sincerely,

Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Hans J. Buitendijk
Vice Chair, EHR Association
Cerner Corporation

HIMSS EHR Association Executive Committee

David J. Bucciferro
Foothold Technology



Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
CPSI

Emily Richmond, MPH
Practice Fusion Inc., a subsidiary of Allscripts

Sasha TerMaat
Epic

Courtney E. Tesvich, RN
Nextech

About the HIMSS EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.