PUBLICATION

Regulatory Sprint: HHS Proposes Expansion of Protections for EHR and Cybersecurity Donations

November 12, 2019

In furtherance of its goals of expanding the adoption of electronic health records (EHR) and improving security through the use of cybersecurity technology, the Department of Health and Human Services (HHS) has proposed expanding protections for EHR and cybersecurity donations. HHS recognizes that barriers (whether real or perceived) to the adoption of EHR and cybersecurity technology will hinder the growth of care coordination which is at the heart of the health care system's move from a volume-based to a value-based system.

The HHS Office of Inspector General (OIG) and the Centers for Medicare & Medicaid Services (CMS) each included two proposals toward that end in their respective proposed coordination of care regulations issued October 2019. First, the OIG and CMS proposed expanding and extending the existing Anti-Kickback Statute (AKS) safe harbor and Physician Self-Referral (Stark) Law exception for EHR donations. Second, the OIG and CMS proposed a new AKS safe harbor and Stark exception for donations of cybersecurity technology and related services. The EHR and cybersecurity proposals are discussed below as part of the Baker Ober Health Law Team's ongoing effort to delve into the details of the Administration's "Regulatory Sprint to Coordinated Care."

EHR Donations Clarifications and Amendments

The OIG and CMS finalized the AKS safe harbor and Stark exception for donations of interoperable EHR software and related training services in 2006, then amended both in 2013. The newly proposed regulations attempt to inject some standardization around the concepts of interoperability, information blocking, and data lock-in. The new regulations also propose the removal of the sunset provisions, offer options with respect to cost-sharing, and clarify protections for cybersecurity technology and software as part of an EHR donation.

Interoperability (deeming provisions, information blocking and data lock-in)

The OIG and CMS propose significant updates to the deeming provisions around the interoperability of EHR software. Currently, the exception and safe harbor deem EHR software as interoperable if the software has been certified before the date of donation. Under the new proposed rules, the donated EHR software must have current certification as of the date of donation. The mere certification of the EHR software at some previous date would no longer qualify under the deeming provision.

The agencies also propose aligning the EHR prohibition against donors who take actions to limit or restrict the use, compatibility, or interoperability of the items or services with other electronic prescribing or EHR systems (now known as information blocking) with the 21st Century Cures Act (Cures Act) definition of *information blocking*. Under the Cures Act, a provider engages in information blocking when the provider "knows that [the] practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of [EHR]." Although health plans are not subject to the information blocking provisions under the Cures Act, the OIG specifically proposes to apply this knowledge standard to both health plans and health care providers.

Cybersecurity

The OIG and CMS also clarify that the EHR safe harbor and exception have always protected certain cybersecurity software and services. The agencies state that an entity donating EHR software and providing training and other related services may also donate the related cybersecurity software and services needed to protect the donated EHR. Individuals seeking protection for cybersecurity software and service donations only need to meet the EHR exception and safe harbor or the newly proposed cybersecurity exception and safe harbor, as discussed below.

Definitions of *Interoperability* and *Electronic Health Records*

The OIG and CMS also propose to modify the definitions of *Electronic Health Records* and *Interoperability* based on the definitions used in the Cures Act and the Office of the National Coordinator for Health Information Technology's proposed regulations.

Cost-sharing/Contribution Requirements

The proposed regulations also seek comments on changing the cost-sharing/contributions requirements. The EHR exception and safe harbor currently require a 15-percent cost-sharing contribution. The OIG and CMS propose three potential alternatives:

- eliminate or reduce the percentage contribution required for small or rural practices;
- eliminate or reduce the 15-percent contribution requirement for all recipients; or
- modify or eliminate the contribution requirement for updates to previously donated EHR software or technology.

Stakeholders are encouraged to submit their comments on the proposed alternatives or other similar alternatives.

Replacement Technology

Both agencies also propose deleting the prohibition against donating equivalent technology, and instead would allow donations of replacement electronic health records technology. The agencies seek comments on this proposal.

OIG's Expanded Scope of Protected Donors

In addition, the OIG proposes expanding the scope of protected donors under the EHR safe harbor to include those who "submit[ ] claims or requests for payment, either directly or through reassignment, to the Federal health care program." In light of its goals to advance the adoption of electronic health records technology, the OIG proposes eliminating or revising the restrictions on who may qualify as a protected donor. If the OIG revises rather than eliminates the provision, it would likely expand the safe harbor protection to entities with indirect responsibility for patient care. This would protect donor entities such as health systems or accountable care organizations that neither are health plans nor submit claims for payment. Notably, CMS made no similar proposal, although it is also not clear that such a change is necessary given the scope of the Stark Law.

Sunset Provision

The current EHR safe harbor and exception are scheduled to end on December 31, 2021. The agencies propose eliminating this sunset provision, although they are also seeking comments on whether a later sunset date should be chosen instead.

Cybersecurity Exception and Safe Harbor

In addition to clarifying that cybersecurity technology and services may be included under the EHR donation exception and safe harbor, the OIG and CMS propose a new, separate cybersecurity technology and services donation exception and safe harbor. The agencies stress the growing threats posed by cyberattacks. Without adequate cybersecurity, these attacks can prevent access to and lead to corruption of health records and other health-related information.

The proposed AKS safe harbor and Stark exception are substantially similar, although there are a few differences which are noted below. For a donation to qualify for the cybersecurity safe harbor or exception, the proposed arrangement must meet the following conditions:

1. The donated technology and/or services must be necessary and must be predominantly used to implement, maintain, or reestablish cybersecurity.

2. Under the Stark exception, the donor cannot condition the donation, the amount or nature of the donation, or the eligibility for donation on referrals or the business generated.

3. Under the AKS safe harbor:

The donor cannot directly take into account the volume or value of referrals or other business between the parties when determining a potential recipient's eligibility for donation, "or the amount or nature of the technology or services to be donated."

The donor cannot condition the donation, the amount or the nature of the donation on future referrals.

4. The potential recipient and/or the potential recipient's practice (including employees or staff members) cannot make the donation of cybersecurity technology and services a condition of doing business or continuing to do business with the donor.

5. The arrangement must be documented in writing, identify the parties to the arrangement, and include a general description of the cybersecurity technology and related service to be donated during the term of the arrangement, the estimated value of the donation, and any shared financial responsibility for the cost of the technology and related services. In addition, under the AKS safe harbor, the written arrangement must be signed by the parties to the arrangement.

6. Under the AKS safe harbor, the donor may not shift the donation costs to federal health care programs.

Newly Defined Terms Under the Cybersecurity Safe Harbor and Exception

The proposed cybersecurity exception and safe harbor include broad definitions for the terms *cybersecurity* and *technology*. The OIG and CMS define *cybersecurity* as "the process of protecting information by preventing, detecting, and responding to cyberattacks." The term *technology* is defined as "any software or other types of information technology other than hardware." It includes:

- cybersecurity software that provides malware prevention; software security measures to protect endpoints that allow for network access control; business continuity software; data protection and encryption; email traffic filtering; and

- cybersecurity services that are associated with developing, installing, and updating cybersecurity software; cybersecurity training services; cybersecurity services for business continuity and data recovery services; "cybersecurity as a service"; cybersecurity risk assessment or analysis; sharing information about known cyber threats; and assisting recipients responding to threats or attacks on their systems.

Although the proposed definition of *technology* excludes hardware, the agencies seek comments on whether to provide limited protection for specific types of hardware. For example, the OIG and CMS raise the possibility of protecting cybersecurity hardware that has been determined reasonably necessary to address identified cybersecurity risks based on the donor's and the potential recipient's cybersecurity risk assessments. The agencies also seek comments on whether to deem certain arrangements as satisfying the requirement that the technology or service is necessary to implement, maintain, or reestablish cybersecurity.

Other Notable Requirements

- The current proposals do not include contribution requirements for donations of cybersecurity technology and services.

- The AKS safe harbor and Stark exception do not protect donations of cybersecurity technology and services that are used in the normal course of the recipient's business (for example, general help desk services).

- All donations must be nonmonetary.

Takeaway

If adopted, the EHR and cybersecurity proposals would open the door to greater use of EHR and cybersecurity technology in the health care industry. Such expansion would also facilitate coordination of care as the health care industry moves from a volume-based to a value-based system. To this end, the proposed regulations appear to have been strategically designed to work congruently with other federal laws and regulations related to health information technology protections.

The OIG and CMS have invited feedback from health care industry stakeholders about a number of important aspects of the EHR and cybersecurity proposals. They seem to genuinely want to make sure these regulations are workable and reflect existing (and, to the extent possible, future) realities of health care IT. Public comments are due by December 31, 2019. Please contact the authors or any other member of Baker Ober Health Law Team for more information about the proposed regulations or submitting comments.