CMS and OIG propose changes to existing rules for donations of electronic health records and new rules for donations of cybersecurity technology and services

November 4, 2019

On October 9, 2019, the Office of Inspector General (OIG) released proposed changes to the regulations interpreting the federal Anti-Kickback Statute (AKS). On the same day, the Centers for Medicare and Medicaid Services (CMS) released proposed changes to the regulations interpreting the Physician Self-Referral Law (Stark Law).

This publication discusses the proposed modifications to the existing AKS safe harbor and Stark Law exception for the donation of electronic health records (EHR) items and services. The proposed changes to the EHR safe harbor and exception are very similar. This publication also discusses the proposed *new* safe harbor and *new* exception for donations of cybersecurity technology and services. While similar in many respects, the proposed new cybersecurity safe harbor and exception contain several material differences.

The cybersecurity exception and safe harbor are broader and include fewer conditions than the EHR exception and safe harbor. However, under the proposed changes, both the EHR exception and safe harbor would be expanded to expressly include cybersecurity software and services, so it is clear that an entity donating EHR software and providing training and other related services may also donate related cybersecurity software and services to protect the EHR. For clarity, both the OIG and CMS would propose to incorporate a definition of "cybersecurity" in the EHR exception/safe harbor that mirrors the definition proposed in the standalone cybersecurity exception/safe harbor. A party seeking protection under the exception and/or safe harbor (as

applicable) needs to comply with the requirements of either the EHR or the cybersecurity exception/safe harbor, not both.

EHR donations

Notable proposed changes to both the EHR exception and safe harbor include:

- Updates to definitions of "interoperable" and "electronic health records" based largely on the terms in the 21st Century Cures Act that update or supersede terms used when the exception and safe harbor were first issued in 2006. The changes are not intended to substantively change the scope of the protection.
- Updates to the deeming provision to clarify that interoperable certification must be current as of the date of the donation, as opposed to the software being certified at some point in the past but no longer maintaining certification as of the date of the donation.
- Updates to the prohibition on taking action to limit or restrict the use, compatibility or interoperability of the items or services with other electronic prescribing or EHR systems. Under the proposed changes, this condition would be aligned with the information blocking definition in the 21st Century Cures Act. This modification, according to the OIG is "not intended to change the purpose of the condition, but instead further our longstanding goal of preventing abusive arrangements that lead to information blocking and referral lock-in through updated understanding of those concepts established by the 21st Century Cures Act."
- Elimination of the concept of an expiration/sunset date for the exception and safe harbor, which is currently set to expire December 31, 2021. As an alternative to the proposed elimination of the sunset provision, the OIG and CMS are seeking comments on whether to keep the sunset date concept.
- Broadening of protections for the donation of software and services related to cybersecurity. Currently, the EHR exception/safe harbor protects EHR software or information technology and training services necessary and used predominantly to create, maintain, transmit or receive EHR. The language would be changed to expressly include certain cybersecurity software and services that "protect" EHR.
- The OIG clarified that certain software and services have always been protected – for instance, a secure login or encrypted access mechanism included with an EHR system or EHR software suite would be considered cybersecurity features of the EHR that are protected under the existing EHR safe harbor.
- While not yet proposing any specific amendment, both the OIG and CMS are considering and soliciting comments on whether to change the requirement that the recipient pay 15 percent of the donor's cost of donated EHR items and services.
- Both CMS and the OIG are considering deleting the condition that prohibits the donation of equivalent items or service to allow donations of replacement EHR technology. Both entities requested comments on the types of situations in which the donation of replacement technology would be appropriate and how to safeguard against inappropriate donations of unnecessary technology.

The OIG is considering expanding the group of entities that may be protected donors under the EHR safe harbor to add entities with indirect responsibilities for patient care. This would include entities such as health systems and accountable care organizations that are not health plans nor submit claims for payment.

Cybersecurity technology and services

The OIG is proposing a new AKS safe harbor, and CMS is proposing a new Stark Law exception, for donations of cybersecurity technology and services. To qualify, both the exception and the safe harbor require that the technology and services are necessary and are used predominantly to implement and maintain effective cybersecurity. Unlike the AKS safe harbor, the Stark Law exception would also protect donations to be used to "reestablish" cybersecurity.

"Cybersecurity" is defined as the process of protecting information by preventing, detecting and responding to cyberattacks. "Technology" is defined as any software or other types of information technology, other than hardware.

Both the cybersecurity exception and the safe harbor would:

- Prohibit eligibility for a donation of cybersecurity technology or services, and the nature or amount of technology or services, from being determined in any manner that directly takes into account the volume or value of referrals or other business generated between the parties.
- Prohibit a recipient of such a donation from making the receipt of the technology or service, or the amount or nature of the technology or service, a condition of doing business with the donor.

Neither the safe harbor nor the exception would require the recipient to contribute to the cost of the donated cybersecurity technology or related services, although such a requirement would not be prohibited.

The Stark Law exception would require that the arrangement be documented in writing. By contrast, the AKS safe harbor would require that the arrangement be set forth in a written agreement that (i) is signed by the parties and (ii) describes the technology and services being provided and the amount of the recipient's contribution, if any.

CMS indicates that while it doesn't require the parties to document the arrangement in a written contract due to concerns that such a requirement would lead to inadvertent violation of the Stark Law, it *does* expect the written documentation of the arrangement to identify the recipient of the donation. That documentation must include a general description of the cybersecurity technology and related services provided to the recipient over the course of the arrangement; the timeframe of donations made under the arrangement; a reasonable estimate of the value of the donation(s); and, if applicable, any financial responsibility for the cost of the cybersecurity technology and related services that is shared by the recipient.

The proposed cybersecurity safe harbor (but not the exception) also contains a provision prohibiting the donor from shifting the costs of the donated technology or services to any federal health care program.

The proposed changes will likely generate many public comments regarding how these proposals will impact real-life arrangements. Public comments on the proposed changes to the regulations interpreting the AKS and Stark Law are due December 31, 2019. As a result, the OIG and CMS will not finalize the proposed changes until 2020.

This publication is part of a series of updates regarding CMS and OIG's proposed fraud and abuse law changes. Bricker & Eckler's health care attorneys will continue to publish analyses of the proposed rule.

Authors