FMVantage Point™
HealthCare Appraisers' Industry Insight

PROPOSED RULE CHANGES FOR CYBERSECURITY IN ELECTRONIC HEALTH RECORD (EHR) DONATION ARRANGEMENTS

DAVID W. SANDS CVA AND FRED LARA, CFA, ASA, CVA

On October 9, 2019, the Centers for Medicare and Medicaid Services (CMS) and the Office of Inspector General (OIG) released new Stark Law and Anti-Kickback Statute (AKS) proposed rules that relate to the donation of cybersecurity technology and services to physicians. The proposed rules, if adopted, will more broadly protect the donation of software and services related to cybersecurity.

The current Stark Law EHR exception (the "EHR Exception") and AKS safe harbor for EHR (the "EHR Safe Harbor") allow a hospital or health system's donation of EHR technology and services to an independent practice. EHR technology and services include software or information technology and training services predominantly used to create, maintain, transmit and/or receive electronic health records. The existing EHR Exception allows for a donation of up to 85% of the cost of such systems, in effect requiring a 15% contribution from the recipients of the EHR technology. The new proposed cybersecurity exception and safe harbor address donation of "cybersecurity technology and services" and will permit non-monetary donations of cybersecurity technology and related services without a 15% contribution by recipients. In addition, CMS and the OIG are proposing to amend the existing EHR Exception and EHR Safe Harbor to clarify that cybersecurity technology and services are covered under the EHR Exception and EHR Safe Harbor as well as under the newly proposed separate cybersecurity exception and safe harbor. The proposed changes to the EHR Exception and EHR Safe Harbor do not include an amendment to the 15% recipient donation requirement, but do request comments on future changes that may:

- Eliminate or reduce the 15% contribution requirement for small or rural practices;
- Eliminate the 15% contribution requirement in its entirety; or
- Modify or eliminate the 15% contribution requirement for updates to previously donated EHR software.

The EHR exception promotes electronic interoperability between providers that is, by nature, subject to cybersecurity concerns. Thus, allowing for the donation of certain cybersecurity technology and services along with EHR further promotes these relationships by eliminating certain cost elements of cybersecurity from the recipient. Included in the guidance for allowed cybersecurity donation are various forms of software and cybersecurity services used primarily for the purposes of implementing and maintaining cybersecurity, though hardware is specifically excluded. Furthermore, services that include the installation, improvement or repair of cybersecurity hardware and/or infrastructure are also excluded. However, during the comment period for the proposed changes (ending on November 27, 2019), certain options are being considered for cybersecurity hardware that is solely utilized for cybersecurity purposes.

The agencies believe that donation of cybersecurity technology is less subject to fraud and abuse risk than donation of EHR technology, and, accordingly, the new proposed Stark Law and AKS rules will not require the recipient (*i.e.*, independent practices) of cybersecurity technology to contribute to any of the donor's (*i.e.*, hospitals and health systems) associated costs (*i.e.*, 100% of the cost of cybersecurity technology may be donated, as opposed to only 85% with respect to EHR systems). Both the Stark Law and AKS proposed rules state that the eligibility of the recipient of the donated cybersecurity technology and associated amount cannot directly consider the volume or value of referrals or other business generated between the parties. Furthermore, the recipient or its practice cannot establish a condition of doing business related to the donation of cybersecurity technology. Donors, however, would not be required to provide cybersecurity technology to all providers that connect to their systems. Instead, they may select recipients based on standards that exclude the consideration of referrals or other related business.

FMV PITFALL

Under existing rules as well as the proposed rules, care must be taken when identifying and quantifying the applicable purpose and costs associated with EHR and cybersecurity technology donation arrangements. Reliance on input from various sources, including EHR vendors and consultants, can help ensure that such factors are established based on an informed, objective and consistent basis. The difference in the allowed donation under the EHR versus cybersecurity donation rules (*i.e.*, 85% for EHR and 100% for cybersecurity technology and services) underscores the importance of accurately categorizing the various elements of EHR and cybersecurity technology that are subject to donation. For more information regarding EHR donation arrangements and related FMV pitfalls, **please see this article** previously published by HealthCare Appraisers.