THE
NATIONAL LAW REVIEW

# New Cybersecurity Donation Safe Harbor and Exception – AKS and Stark Final Rule

Article By
Timothy Cahill
Jared M. Bruce
Dinsmore & Shohl LLP
Publications

- Administrative & Regulatory
- Corporate & Business Organizations
- Health Law & Managed Care
- Election Law / Legislative News

- All Federal

Tuesday, December 8, 2020

On Nov. 20, 2020, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) and the Centers for Medicare and Medicaid Services (CMS) issued two final rules, which implement changes to the Physician Self-Referral Law (Stark Law) and the Anti-Kickback Statute (AKS) regulations (respectively the CMS Final Rule and the OIG Final Rule, collectively the Final Rules). This alert is a part of our ongoing summary of the Final Rules.

The Final Rules include the addition of a new "cybersecurity exception" to the general prohibition on payment of any form of remuneration to induce or encourage patient referrals. Accordingly, the OIG Final Rule excludes a new AKS safe harbor to promote the donation of certain cybersecurity technology. The CMS Final Rule includes a new exception to also address the donation of cybersecurity technology. Additionally, the CMS Final Rule modifies the existing Stark Law exceptions for electronic health records (EHR). The overall goal of the new Stark exception and AKS Safe Harbor is to reduce harm from cyber threats in the health care industry. For example, HHS suggests that under the Final Rules, health systems will be specifically permitted to donate cybersecurity technology to individual physician practices to help strengthen the health care industry against the threat of

cyberattacks.

## New AKS Safe Harbor for Donation of Cybersecurity Technology and Related Services

The OIG Final Rule contains a new AKS safe harbor to permit non-monetary donations of certain cybersecurity technology, related services and associated hardware. To qualify for safe harbor protection, the donations must, among other things, be "necessary and used predominantly to implement, maintain, or re-establish effective cybersecurity."[1] The parties must codify the terms of the donation in writing, such as the scope of the donation and the parties' responsibilities (including any contribution required by the recipient of the donation). The OIG made clear in the Final Rule that donors may not directly take into account the volume or value of referrals or other business generated between the parties or the amount or nature of the technology or services to be donated when determining the eligibility of a potential recipient for donated technology or services.

The OIG decided not to include several requirements or limitations within the OIG Final Rule that were under consideration in the OIG proposed rule. One such change from the OIG proposed rule was the removal of a monetary cap or a requirement that the recipient of the donation contribute to the overall cost of cybersecurity technology or services. The OIG also made a modification to the OIG proposed rule when it decided not to limit or restrict the types of individuals or entities eligible to be donors or recipients and not to categorically exclude hardware from the safe harbor's protection. Further, the OIG is not requiring a risk assessment for hardware donations.

## Changes to Stark Law Exceptions for Electronic Health Record Systems

The CMS Final Rule included changes to existing EHR exception provisions, clarifying that cybersecurity software and service donations are permitted, removing the Dec. 31, 2021 sunset provision, and modifying the definitions of "EHR" and "interoperable." CMS also modified the 15 percent physician contribution requirement (but did not eliminate it) and will allow certain donations of replacement technology.

After reviewing the comments on the CMS proposed rule, CMS decided to expand the EHR exception to expressly include cybersecurity software and services so that it is clear that an entity donating EHR software and providing training and other related services may also utilize the EHR exception to protect donations of related cybersecurity software and services to protect the EHR system, provided that all the requirements of the EHR exception are satisfied. In the CMS Final Rule, CMS removed the word "certain" before "cybersecurity software and services" in the introductory paragraph to avoid ambiguity regarding the scope of the EHR exception. CMS indicated that the intent behind this change from the CMS proposed rule was to apply the scope broadly to all related cybersecurity services that would be donated and "necessary and used predominantly" to implement an effective cybersecurity

program.

CMS chose not to finalize a proposed information-blocking exception to the Stark Law in the proposed CMS rule, stating that more recent authorities, such as the Office of the National Coordinator for Health Information, are better suited to enforce the prohibition against information blocking.

## New Stark Law Exception for Donation of Cybersecurity Technology and Related Services

Similar to the new AKS safe harbor for the donation of cybersecurity and related services, the CMS Final Rule included a new exception to protect nonmonetary remuneration that consists of cybersecurity technology and related services that are necessary and used predominantly to implement, maintain, and re-establish effective cybersecurity. In order to qualify for this exception, the cybersecurity technology donation agreement must be in writing, the physician's eligibility for the donation must not be determined in any manner that takes into account the volume or value of referrals or other business generated between the parties, and other requirements. Unlike the existing Stark exception for EHR, there is no requirement for the physicians to share in the cost of such hardware or software.

## Key Takeaway

HHS and CMS have specifically created an AKS safe harbor and Stark law exception that promote access to cybersecurity technology. Health care systems will be able to provide other health care providers, such as individual physician practices, with cybersecurity solutions as donations as long as certain requirements that protect against fraud and abuse are met. Through the new AKS safe harbor and Stark law exception, HHS seeks to promote the use and donation of cybersecurity technology which, in turn, should result in a more robust cybersecurity framework for the entire health care industry.

[1] 42 C.F.R. § 411.357(bb).



---

National Law Review, Volume X, Number 343