Cybersecurity Technology and Services Stark Law Exceptions and Anti-Kickback Safe Harbors; Updates to EHR Donation Rules

Cybersecurity Technology and Services

In recognition of its growing importance, the existing Electronic Health Records exception[1] and safe harbor[2] now permit the donation of specified cybersecurity software and services.

There is also a new AKS safe harbor[3] and a virtually identical Stark Law exception[4] that protect non-monetary remuneration of cybersecurity technology and services that are necessary and used predominantly to implement, maintain or reestablish effective cybersecurity if: (1) the donor does not directly consider volume or value of referrals when setting eligibility of potential recipients or the amount of donated technology; (2) the donation is not conditioned on doing business with the donor; (3) the arrangement is documented in writing; and (4) the donor does not shift costs of the technology or services to any Federal Health Care Program.

Changes to EHR Donation Rules

The final rules include changes to the Anti-Kickback Statute and the Stark Law regulations applicable to electronic health records (EHR) items and services. Below is a summary of the key changes that are being finalized:

- Sunset Date Eliminated. The December 31, 2021, sunset date for the EHR Exception and Safe Harbor is eliminated under both final rules. Accordingly, the EHR Exception and Safe Harbor are now permanent.
- The "No Equivalent Technology" Requirement Has Been Eliminated. In order to receive protection under the original EHR Exception and Safe Harbor, the recipient of donated EHR items and services could not possess technology that was "equivalent" to those being donated. The Final Rules eliminate this requirement. Replacement technology will now be treated the same as a new donation and will need to meet all the requirements of the safe harbor and exception to receive protection.
- 15% Contribution Requirement Remains in Effect. Under the original EHR Exception and Safe Harbor, a recipient of a donated EHR had to contribute at least 15% of the cost of the EHR. When the OIG and CMS issued their Proposed

[1] 42 C.F.R. Section 411.357 (w).
[2] 42 C.F.R. Section 1001.952 (y).
[3] 42 C.F.R. Section 1001.952 (jj).
[4] 42 C.F.R. Section 411.357 (bb).

Rules, they solicited comments on alternatives regarding to the original 15% contribution requirement. In the Final Rules, the OIG and CMS eliminated the requirement that the 15% contribution be paid in advance for *updates to previously donated* EHR software and technology. CMS clarifies that these payments must be made "at reasonable intervals." However, recipients of donated EHR items and services, whether provided as *first-time EHR technology or replacement EHR technology*, must still pay the required 15% contribution *in advance* of the initial donation.

- Expanded List of "Protected Donors." The final EHR Exception and Safe Harbor expand the list of the types of entities that can be donors. While the original rules required permissible donors to be eligible for enrollment in Medicare or other federal health care programs, the types of entities that are permissible donors under the Final Rules also include entities comprised of organizations that enroll or provide services and submit claims to a Federal health care program. Accordingly, this expansion allows entities such as parent companies of hospitals, health systems, and accountable care organizations (ACOs) to serve as permissible donors.
- Donation of Cybersecurity Software and Services. CMS and OIG clarified that cybersecurity software and services fit within the EHR Exception and Safe Harbor so long as the donated cybersecurity items or services are necessary and used predominately to protect health records, and additionally that all other requirements of the EHR Exception and Safe Harbor are met. Also within the Final Rules, the OIG and CMS each published a separate new Cybersecurity Technology and Related Services AKS Safe Harbor and Cybersecurity Technology and Related Services Stark Law Exception (collectively, the Cybersecurity Exception and Safe Harbor). The new Cybersecurity Exception and Safe Harbor are broader in scope. Unlike the EHR Exception and Safe Harbor, there are no contribution requirements for the software, services, and hardware that qualify for donation under the Cybersecurity Exception and Safe Harbor.
- Interoperability. Interoperability continues to be required for donated EHR items and services. The EHR Exception and Safe Harbor clarify the meaning of "interoperable." Under the Final Rules, "interoperable" means able to both:
    - Securely exchange data with and use data from other health information technology
    - Allow for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law.

In the Final Rules, CMS and OIG explain that it is deemed interoperable if on the date it is provided to the recipient, it is certified by a certifying body authorized by the National Coordinator for Health Information Technology (ONC) to certification

criteria identified under the then-applicable federal regulations (currently 45 CFR part 170). ONC-approved certification is not the only way to meet the interoperability standard, but having such certification will provide assurance that the software is deemed interoperable.