Services

Expanded Availability of Anti-Kickback Statute Safe Harbors

The U.S. Department of Health and Human Services, Office of Inspector General ("OIG") published the Medicare and State Health Care Programs; Fraud and Abuse; Revisions to Safe Harbors under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements Final Rule (the "AKS Final Rule"), which revises regulations implementing the Federal Anti-Kickback statute (the "AKS"). The published AKS Final Rule can be found here. The AKS Final Rule is effective January 19, 2021. The AKS Final Rule offers greater flexibility in existing AKS safe harbors and creates new safe harbors available for individuals and entities who desire to receive safe harbor protection.

The following is a summary of the AKS Final Rule.

Personal Services and Management Contracts Safe Harbor ("Personal Services Safe Harbor")

The AKS Final Rule revises the Personal Services Safe Harbor[1] in the following manner:

- It removes the requirement that an agreement for periodic, sporadic, or part-time services specify exactly the schedule of intervals during which services will be provided, their precise length, and the exact change for such intervals; and
- It removes the requirement that the aggregate compensation for the services be stated in the agreement; instead, the methodology for determining the compensation must be defined in the agreement.

These two revisions will allow more agreements that historically would not have qualified for safe harbor protection, to meet the requirements of the Personal Services Safe Harbor. Agreements such as medical director services agreements and call coverage agreements, which usually present a low risk of abuse, will now (assuming they meet the requirements of the revised Personal Services Safe Harbor) fit within the safe harbor, and parties to the arrangement will not have to rely on a facts and circumstances AKS analysis.

Added to the Personal Services Safe Harbor is a new exception for certain outcomes-based payments. An in-depth discussion of this addition is available here.

1. 42 C.F.R. 1001.952(d).

Warranties Safe Harbor

The Warranties Safe Harbor[2] is modified such that the definition of "warranty" includes warranties for bundled items and related services rather than only single-item warranties.

In recognition of the concern expressed in OIG Advisory Opinion 18-10, which said warranty arrangements involving a bundle of items that were separately reimbursable could result in overutilization of one or more items included in the bundle and could unnecessarily increase costs to Federal health care programs, OIG has also added a requirement that a warranty for more than one item, or for one or more items and related services, can only cover items and services reimbursed under the same Federal health care program and in the same program payment. This, for example, would preclude bundled-item warranty arrangements where one of the warrantied items was reimbursable under the hospital prospective payment system and another warrantied item in the bundle was reimbursed under the Medicare physician fee schedule. Note that the OIG has expressly stated that this requirement does not prohibit the inclusion of non-federally reimbursable items or services in the bundle of items and services being warrantied. For example, a manufacturer could offer a bundled warranty that warranties the clinical effectiveness of a self-injected drug contingent on the patient receiving post-prescribing product administration and use education through nurse support offered by the manufacturer.

Additionally, warranties may not be conditioned on a buyer's exclusive use of, or minimum purchase of, the manufacturer's or supplier's items or services. The OIG has explained that while exclusivity and minimum-purchase requirements may allow for certain efficiencies, tying a warranty to exclusivity and minimum purchase requirements could result in interference with clinical decision-making, overutilization or inappropriate utilization, or anticompetitive effects. However, the revised safe harbor protects warranties in which a bundle of items or a bundle of items and services must be used together to obtain warranty protection.

Electronic Health Records Items and Services Safe Harbor ("EHR Safe Harbor")

The AKS Final Rule made a number of changes to the EHR Safe Harbor.[3] First, consistent with the new cybersecurity technology and related services safe harbor, the EHR Safe Harbor now specifically allows the provision of cybersecurity software and services to fit within the safe harbor.

An additional change to the EHR Safe Harbor is seen in the requirement regarding the recipient's contribution to the cost of the EHR. While the recipient of EHR support must still pay 15% of the donor's cost of the items and services, the requirement that the payment be made in advance of receiving items or services now applies only to the initial donation of EHR items and services or the replacement of part or all of the existing EHR system. A contribution for updates to previously donated EHR items and services need not be paid in advance of receiving the update.

Further updates to the EHR Safe Harbor include removal of the sunset provision, which previously required that EHR be provided and all conditions to satisfy the safe harbor be met on or before December 31, 2021, and removal of the prohibition on providing equivalent technology.

2. 42 C.F.R. 1001.952(g).
3. 42 C.F.R. 1001.952(y).

Local Transportation Safe Harbor

The AKS Final Rule modifies the Local Transportation Safe Harbor[4] to increase from 50 miles to 75 miles the radius for free or discounted transportation (including by a ride-sharing service or other means of local transportation that may exist in the future) for patients residing in a rural area. Additionally, if a patient is discharged from an inpatient facility following inpatient admission or released from a hospital after being placed in observation status for at least 24 hours and transported to the patient's residence or another residence of the patient's choice, the mileage limits do not apply. The OIG reiterated that a residence may include (1) a custodial care facility that serves as a patient's permanent or long-term residence if the patient established the facility as a residence before receiving treatment by the facility from which the patient is being transported, (2) a homeless shelter when a patient is homeless or established the homeless shelter as a residence prior to hospital admission, and (3) the residence of a friend or relative who is caring for the patient post-discharge.

The OIG reminds providers that they are responsible for ensuring that transportation service providers comply with the prohibitions against luxury transportation and public marketing or advertising of the free or discounted local transportation services. While a transportation services provider can generally make known that it provides transportation to medical appointments and suggest to patients that they contact their medical providers to see whether the provider offers free or discounted transportation, the transportation services provider cannot identify particular health care providers with which it partners to provide transportation. Such action by the transportation services provider would be imputed to the healthcare provider.

The OIG declined to extend protection under the Local Transportation Safe Harbor to transportation for non-medical health-related purposes.

Cybersecurity Technology and Related Services Safe Harbor ("Cybersecurity Safe Harbor")

The AKS Final Rule created the Cybersecurity Safe Harbor[5] which protects arrangements that are intended to address the growing threat of cyberattacks impacting the health care ecosystem that comply with the terms of the Cybersecurity Safe Harbor from risk of liability under the AKS. Contemporaneous with the publication of the AKS Final Rule, the Centers for Medicare & Medicaid Services ("CMS") published the Stark Law Final Rule,[6] which established an exception to the Stark Law's referral and billing prohibitions for cybersecurity technology and related services (the "Cybersecurity Exception").[7] The Cybersecurity Safe Harbor and Cybersecurity Exception are substantively similar[8] and protect the donation of software and other types of information technology, including hardware that meet the conditions of the Cybersecurity Safe Harbor or Cybersecurity Exception, as applicable.

Pursuant to the AKS Final Rule and Stark Law Final Rule, the use or sharing of cybersecurity items and services may be available under the value-based purposes safe harbors and exceptions (as further discussed in our separate white paper), included in the donation of electronic health records items and services pursuant to the applicable Stark Law exception or EHR Safe Harbor,[9] or protected under the new Cybersecurity Safe Harbor and Cybersecurity Exception.

4. 42 C.F.R. 1001.952(bb).
5. 42 C.F.R. 1001.952(jj).
6. 85 Fed. Reg. 77492 (Dec. 2, 2020) (the "Stark Law Final Rule"). A summary of the Stark Law Final Rule can be found at [insert link to Chris's summary].
7. 42 C.F.R. 411.357(bb).
8. 85 F.R. 77492, 77630 (stating, "Despite the differences in the respective underlying statutes, we attempted to ensure as much consistency as possible between the exception to the physician self-referral law and the safe harbor to the anti-kickback statute.")
9. 42 C.F.R. 411.357(w); 42 C.F.R. 1001.952(y).

Generally, the Cybersecurity Safe Harbor and separate Cybersecurity Exception protect nonmonetary remuneration, including cybersecurity[10] technology[11] and services that are necessary and used predominantly to implement, maintain, or reestablish cybersecurity,[12] provided:

1. The donor does not (i) directly take into account the volume or value of referrals or other business generated between the parties when determining the recipient's eligibility or the amount or nature of the technology or services to be donated or (ii) condition the donation on future referrals;
2. The recipient does not make the receipt of technology or services, or the amount or nature of the technology or services, a condition of doing business with the donor; and
3. A general description of the technology and services and the amount of the recipient's contribution, if any, are set forth in writing.[13]

The Cybersecurity Safe Harbor and Cybersecurity Exception are available to all types of individuals and entities, in contrast to other AKS safe harbors and Stark Law exceptions which are available to limited groups.[14] While neither the Cybersecurity Safe Harbor nor the Cybersecurity Exception require a clear nexus between the donation and the business relationship, both require that the donation be necessary.[15]

In addition to being necessary, the cybersecurity technology and services must be used *predominantly* for cybersecurity. Technology and services, including software, that have multiple functions, one of which is cybersecurity, likely would not meet the necessary and predominant use standards of the Cybersecurity Safe Harbor and Cybersecurity Exception unless the software's predominant function is for cybersecurity.

The following were identified by the OIG and CMS as examples of services that the OIG and CMS believe would be necessary and used predominantly to implement, maintain, or reestablish cybersecurity:

- Any services associated with developing, installing, and updating cybersecurity software;
- Any kind of cybersecurity training services, such as training recipients how to use cybersecurity technology, how to prevent, detect, and respond to cyber threats, and how to troubleshoot problems with the cybersecurity technology (e.g., "help desk" services specific to cybersecurity); and
- Any kind of cybersecurity services for business continuity and data recovery services to ensure the recipient's operations can continue during and after a cyberattack.

---

10. *Cybersecurity* means the process of protecting information by preventing, detecting, and responding to cyberattacks. 42 C.F.R. 1001.952(jj)(5)(i). Identical definition for purposes of the Cybersecurity Exception to the Stark Law at 42 C.F.R. 411.351.
11. *Technology* means any software or other types of information technology. 42 C.F.R. 1001.952(jj)(5)(ii). Identical definition for purposes of the Cybersecurity Exception to the Stark Law at 42 C.F.R. 411.357(bb).
12. The Cybersecurity Safe Harbor also requires that the donation be for effective cybersecurity; whereas, CMS specifically declined to include a requirement that the donation be effective. See 85 F.R. 77492, 77636 (stating, "In the strict liability context of the physician self-referral law, we are concerned that requiring 'effective' cybersecurity at 411.357(bb)(1) may chill otherwise beneficial cybersecurity donations, as donors and recipients may lack the expertise to understand and determine what constitutes 'effective' cybersecurity or there may be disagreement as to whether cybersecurity measures are 'effective'.")
13. The Cybersecurity Safe Harbor also includes a signature requirement and requires that the donor not shift costs of the technology or services to any Federal health care program.
14. *See* the Electronic health records items and services safe harbor at 42 C.F.R. 1001.952(y) and the Electronic health records items and services exception at 42 C.F.R. 411.357(w).
15. *See* 85 F.R. 77684, 77816 (stating, "It is unlikely that a donation would be necessary for the donor or recipient to implement, maintain, or reestablish effective cybersecurity if it is not connected to the underlying services furnished by either party (e.g., ensuring the secure transfer of information between the parties.)").

Provided all requirements of the Cybersecurity Safe Harbor or Cybersecurity Exception are met, the following technology would be permitted: computer privacy screens, two-factor authentication dongles, security tokens, facial-recognition cameras for secure access, biometric authentication, secure identification card and device readers, intrusion detection systems, data backup, and data recovery systems.[16]

As finalized, the Cybersecurity Safe Harbor permits the donor to furnish the services on its own or under contract with a third party. Additionally, while donors are free to require recipients to contribute to the costs of donated cybersecurity technology and services, as long as the determination of a contribution requirement or the amount of the contribution does not take into account the volume or value of referrals or other business generated, neither the Cybersecurity Safe Harbor nor the Cybersecurity Exception require the recipient to contribute to the costs of the donated technology or services.

Notably, the Cybersecurity Safe Harbor and Cybersecurity Exception do not require that the parties perform a risk assessment prior to donating the technology or services;[17] there is no requirement that donations meet specific standards to protect patient data from cyberattacks or threats; and there is no monetary cap. However, the Cybersecurity Safe Harbor and Cybersecurity Exception do not protect donations of cash or cash-equivalents to purchase cybersecurity technology or services, to reimburse for the purchase of cybersecurity technology or services, or to cover fines, ransom or litigation stemming from a cyberattack. Additionally, neither the Cybersecurity Safe Harbor nor the Cybersecurity Exception provide any immunity from risk of cybersecurity incidents for the donors.

As with all AKS safe harbors, complying with the Cybersecurity Safe Harbor is not mandatory, but is available to parties who desire to fall under its protection from potential risk under the Federal AKS and compliance with a Stark Law exception, including the Cybersecurity Exception, is only required for individuals or entities subject to the Stark Law.

Value-Based Arrangements

The AKS Final Rule also contains new safe harbors for certain value-based arrangements. These are addressed separately here.

Civil Money Penalties Act

The AKS Final Rule codifies, as part of the Civil Money Penalties Act, the statutory exception for "telehealth technologies" furnished to certain in-home dialysis patients. Under the new rule, remuneration does not include, for purposes of the civil monetary penalty beneficiary inducement rule, the provision of telehealth technologies by a provider of services, physician, or renal dialysis facility to an individual with end-stage renal disease who is receiving home dialysis for which payment is made under Medicare Part B if (1) the telehealth technologies are furnished to the individual by the provider of services, physician, or the renal dialysis facility that is currently providing the in-home dialysis, telehealth services, or other end-stage renal disease care to the individual, or has been selected or contracted by the individual to schedule an appointment or provide services; (2) the telehealth technologies are not offered as part of

16. The following hardware likely would not qualify for the Cybersecurity Safe Harbor or Cybersecurity Exception as either (i) failing to satisfy the pre-dominant use standard or (ii) not meeting the definition of "technology": servers, drives, locks on doors, upgraded wiring, physical security systems, fire retardant or warning technology, and high-security doors.
17. While not required, a risk assessment could be used to demonstrate that the donation is necessary.

any advertisement or solicitation; and (3) the telehealth technologies are provided for the purpose of furnishing telehealth services related to the individual's end-stage renal disease.

Telehealth technologies include hardware, software, and services that support distant or remote communication between the patient and provider, physician, or renal dialysis facility for diagnosis, intervention, or ongoing care management.

If you have questions regarding the AKS Final Rule, please reach out to a member of Kutak Rock's National Healthcare Practice Group.