ADVISORIES

Healthcare

Sprint Regulations: EHR and Cybersecurity Proposals

By Caitlin Forsyth, Adam H. Greene, and Gavin Keene

10.28.19

Consistent with the Administration's broader effort to reduce regulatory burdens within the healthcare industry, the Sprint Regulations include proposals designed to remove barriers to the widespread adoption of cybersecurity technology. The proposals reflect a prescient recognition that any system-wide evolution toward integration cannot occur without investments in what OIG calls "cybersecurity hygiene."

To that end, CMS and OIG have offered (i) proposed modifications to the existing anti-kickback statute (AKS) safe harbor and Stark Law exception for the donation of electronic health records (EHR) technology and services, and (ii) a proposed new Stark exception and AKS safe harbor for the donation of cybersecurity technology and related services.

These proposals are described in more detail below.

1. Stark EHR Donation Exception (42 C.F.R. § 411.357(w)) and AKS Safe Harbor (42 C.F.R. § 1001.952(y))

In August 2006, CMS and OIG finalized a Stark exception and an AKS safe harbor for certain arrangements involving the donation of interoperable electronic health record (EHR) software or information technology and training services. The initial EHR donation exception and safe harbor were scheduled to expire on December 31, 2013.

In December 2013, CMS and OIG published final rules extending the expiration dates to December 31, 2021, excluding laboratories, and updating the provision under which EHR software is deemed interoperable (the "Deeming Provision").

CMS and OIG now propose parallel updates to this exception and safe harbor, reinterpreting concepts around interoperability and data lock-in, clarifying that donations of certain cybersecurity software and services are permitted, removing the sunset provision, and modifying the definitions of "electronic health record" and "interoperable."

Interoperability

Under the Deeming Provision, software is currently deemed to be interoperable if on the date it is provided to the physician it has been certified by a certifying body to an edition of the EHR certification criteria identified in the then-applicable version of 45 CFR part 170. CMS and OIG propose two textual clarifications:

- First, the agencies propose to modify the language to clarify that the certification must be current as of the date of the donation, as opposed to the software having been certified at some point in the past but no longer maintaining certification on the date of the donation.

- Second, they propose to remove the reference to "an edition" of the EHR certification criteria to align with proposed changes to the ONC's certification program.

The current version of the exception and safe harbor prohibits the donor (or any person on the donor's behalf) from taking any action to limit or restrict the use, compatibility, or interoperability of the items or services with other electronic prescribing or EHR systems. Since the publication of CMS's and OIG's final rules, significant federal government action, including through amendment of the Public Health Service Act (PHSA), has defined conduct that would be characterized as "information blocking."

Thus, CMS proposes modifications to prohibit the donor (or any person on the donor's behalf) from engaging in a practice constituting information blocking, as defined in section 3022 of the PHSA. OIG takes a slightly different approach, proposing modifications to the safe harbor to prohibit the donor from engaging in a practice constituting information blocking, as defined in 45 CFR Part 171.

Cybersecurity

CMS and OIG also propose an amendment to the EHR exception and safe harbor to clarify that protection is available (and always has been available) for certain cybersecurity software and services.

While the agencies are also proposing a new exception and safe harbor specifically to protect arrangements involving the donation of cybersecurity technology and related services (the "cybersecurity exception"), discussed below, the expansion of the EHR exception and safe harbor to expressly include certain cybersecurity software and services is intended to make it clear that an entity donating EHR software may also donate related cybersecurity software and services to protect the EHR.

Sunset Provision

The Sprint Regulations propose to eliminate or, in the alternative, extend the sunset provisions in the Stark exception and the AKS safe harbor.

Definitions

CMS proposes to update the definition of "interoperable" to align with the statutory definition of "interoperability" added by the 21st Century Cures Act ("Cures Act") to section 3000(9) of the PHSA. CMS proposes to define "interoperable" to mean:

> (i) Able to securely exchange data with and use data from other health information technology without special effort on the part of the user;
>
> (ii) Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
>
> (iii) Does not constitute information blocking as defined in section 3022 of the PHSA.

OIG proposes an identical update to the definition of "interoperable," except it refers to the definition of information blocking in 45 CFR Part 171 rather than Section 3022 of the PHSA.

Additional Proposals and Considerations

Currently, the EHR exception requires the physician to pay 15 percent of the donor's cost of the technology. Responding to comments indicating that the 15 percent contribution has proven burdensome to some recipients and acts as a barrier to the adoption of EHR technology, CMS and OIG are soliciting comments on two alternatives.

First, the agencies are considering eliminating or reducing the percentage contribution required for small or rural physician organizations. In the alternative, the agencies are considering reducing or eliminating the 15 percent contribution requirement for all physician recipients.

CMS and OIG are also proposing to permit donations of replacement technology. This proposal responds to concerns that the current prohibition on donations of equivalent technology locks physician practices into a vendor, even if they are dissatisfied with the technology. In effect the recipient must choose between paying full cost for a new "replacement" system or continuing to pay 15 percent of the cost of upgrades or additions to their current system.

2. Donations of Cybersecurity Technology and Services: Proposed Stark Exception (42

C.F.R. § 411.357(bb)) and AKS Safe Harbor (42 C.F.R. § 1001.952(jj))

CMS and OIG both propose to protect the donation of certain cybersecurity technology and related services. The Stark exception and AKS safe harbor are substantially similar.

CMS and OIG acknowledge prevalence of cyberattacks, the dramatic increase in the cost of cybersecurity technology and the failure of many providers to invest in cybersecurity measures. Further, the Sprint Regulations commentary notes that one of the key motivators for donors to provide cybersecurity technology and related services is to protect themselves (the donors) from cyberattacks.

The risks associated with a cyberattack on a single provider or supplier in an interconnected system are ultimately borne by every player in the system, so any hospital or other entity wishing to protect itself from cyberattacks has a vested interest in ensuring that the physicians with whom the entity shares data are also protected.

Under the new exception and safe harbor, donations of cybersecurity technology and related services would be protected if all of the following conditions are met (conditions unique to each law are designated as such):

1. The technology and services are necessary and used predominantly to implement, maintain, or reestablish cybersecurity.

2. (*Stark*) Neither the eligibility of a physician for the technology or services nor the amount or nature of the technology or services is determined in any manner that directly takes into account the volume or value of referrals or other business generated between the parties.

   (*AKS*) 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 eligibility of a potential recipient for the

technology or services, or the amount or nature of the technology or services to be donated; or

ii. Condition the donation of technology or services or the amount or nature of the technology or services to be donated on future referrals.

3. Neither the physician nor the physician's practice (including employees and staff members) makes the receipt of technology or services or the amount or nature of the technology or services a condition of doing business with the donor.

4. The arrangement is documented in writing.

   i. (*AKS*) The writing is (i) signed by the parties and (ii) describes the technology and services being provided and the amount of the recipient's contribution, if any.

5. (*AKS*) The donor does not shift the costs of the technology or services to any federal healthcare program.

Definition of Cybersecurity

The Sprint Regulations define cybersecurity broadly, deriving the definition from the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure. Under the Stark exception and AKS safe harbor, Cybersecurity will mean "the process of protecting information by preventing, detecting, and responding to cyberattacks."

Definition of Technology

The Sprint Regulations broadly define technology to include cybersecurity software and other IT, such as an Application Programming Interface (API) which is neither software nor a service as those terms are generally used. Importantly, the definition of technology excludes hardware, given the agencies' concern that donations of valuable, multifunctional hardware poses a higher risk than software of constituting a disguised payment for referrals.

However, both agencies are soliciting comment on whether certain types of hardware should be permitted.

Conditions on Donation and Protected Donors

The donated technology and services must be necessary and used predominantly to implement, maintain, or reestablish cybersecurity. CMS and OIG, however, are taking a neutral position with respect to the types of technology and services covered by the exception and safe harbor, offering a non-exhaustive list of examples.

The types of technology potentially protected under the proposed exception include software that provides malware prevention, software security measures to protect endpoints that allow for network access control, business continuity software, data protection and encryption, and email traffic filtering.

CMS and OIG also proposes to protect a broad range of services, including:

- Services associated with developing, installing, and updating cybersecurity software;
- Cybersecurity training services, such as training recipients on how to use the cybersecurity technology, how to prevent, detect, and respond to cyber threats, and how to troubleshoot problems with the cybersecurity technology (for example, "help desk" services specific to cybersecurity);
- Cybersecurity services for business continuity and data recovery services to ensure the recipient's operations can continue during and after a cybersecurity attack;
- "Cybersecurity as a service" models that rely on a third-party service provider to manage, monitor, or operate cybersecurity of a recipient;
- Services associated with performing a cybersecurity risk assessment or analysis, vulnerability analysis, or penetration test; and
- Services associated with sharing information about known cyberthreats, and assisting recipients responding to threats or attacks on their systems.

The exception would not protect donations of technology and services that are otherwise used in the normal course of the recipient's business (e.g., general help desk services). In all cases, donations must be nonmonetary.

CMS and OIG are seeking comment on whether certain arrangements should be deemed to satisfy the requirement that the technology or services be necessary to implement, maintain, or reestablish cybersecurity. The deeming provision would not affect the requirement that the technology or services be used predominantly to implement, maintain, or reestablish cybersecurity. Parties would have to show on a case-by-case basis that this requirement is met.

No Recipient Contribution
CMS and OIG are not proposing to require recipients to contribute any portion or percentage of the cost of the cybersecurity technology or related services.

Written Documentation
The Sprint Regulations require written documentation of the donation arrangement identifying the recipient of the donation and including a general description of the cybersecurity technology and related services, the timeframe of donations, a reasonable estimate of the value, and, if applicable, any financial responsibility for the cost of the cybersecurity technology and related services.

CMS's proposed exception does not require the parties to document the arrangement in a signed contract, but notably OIG's safe harbor does impose this requirement.

Alternative Proposal
CMS solicits comments on an alternative approach that would allow the donation of cybersecurity hardware. Under this alternative proposal, a protected donation could also include cybersecurity hardware if both the donor and the recipient undertake cybersecurity risk assessments that support the donation of the hardware as a reasonable means to address an identified risk or threat.

Both risk assessments must be conducted in a manner consistent with industry standards.

Takeaways

- The Sprint Regulations include meaningful proposals to reduce the compliance burden associated with the adoption and donation of cybersecurity. The proposals include expanding the existing Stark

exception and AKS safe harbor for EHR donations, creating a new Stark exception and AKS safe harbor for donations of cybersecurity technology, and harmonizing the fraud and abuse laws with existing laws governing technology (e.g., the PHSA and the Cures Act).

- If the Sprint Regulations are finalized, healthcare entities should be able to take comfort in offering cybersecurity software to physicians within the confines of the new rules. CMS and OIG recognize the value to all parties of the widespread adoption of cybersecurity and, within limits, are less concerned about improper financial incentives in cybersecurity donation arrangements.
- Comments on the Sprint Regulations must be submitted by December 31, 2019. CMS and OIG signal throughout the proposed rules that they welcome stakeholder feedback to ensure that the rulemaking is both effective and practical.

Related Articles

11.27.19
ADVISORIES
Healthcare

CMS Finalizes Hospital Pricing Transparency Rule

10.28.19
ADVISORIES
Healthcare

Sprint Regulations: Value-Based Stark Exception and AKS Safe Harbors

10.28.19
ADVISORIES
Healthcare

The Other Half of the Stark Sprint Regulations - Valuable (but Not Value-Based) Proposals