Health Information Compliance Alert

Policy: Stark and AKS Updates Promote IT, Cybersecurity

See new safe harbors on technical donations.

A few months ago, the feds announced they were going to wait an extra year before finalizing long-awaited kickback policies - many related to health IT. In a shockingly quick turnaround, they've fast-tracked final rules with effective dates next month.

Backtrack: In October 2019, the **HHS Office of Inspector General** (OIG) published proposed rulemaking as part of the "HHS Regulatory Sprint to Coordinated Care" impacting Civil Monetary Penalties (CMPs) and the Anti-Kickback Statute (AKS). The **Centers for Medicare & Medicaid Services** (CMS) also suggested updates to the Physician Self-Referral Law - Stark Law for short - modernizing many of its policies to address technology, value-based care, and compensation. Additionally, all the changes aimed to cut administrative burdens, align with other mandates like the 21st Century Cures Act, and improve care coordination across the healthcare spectrum.

Originally, the final rules were promised in August 2020. However, on Aug. 27, CMS released an extension on the Stark final rule in the Federal Register, delaying its release until 2021. OIG did not announce a new date, but most assumed the agency would also push out the AKS and CMP final rule.

Now: On Nov. 20, the two agencies surprised providers with a holiday gift - final rules on the Stark Law, AKS, and CMPs. The rules were published in the Federal Register on Dec. 2.

"When we kicked off our Patients Over Paperwork initiative in 2017, we heard repeatedly from front-line providers that our outdated Stark regulations saddled them with costly administrative burden and hindered value-based payment arrangements," said CMS Administrator **Seema Verma** in a release. "That sound you hear is the mingled cheers and exclamations of relief from doctors and other healthcare professionals across the county as we lift the weight of our punishing bureaucracy from their backs."

Principal Deputy Inspector General **Christi A. Grimm** reiterates Verma's excitement. "OIG's new safe harbor regulations are designed to facilitate better coordinated care for patients, value-based care, and improved cybersecurity, while also protecting against fraudulent or abusive conduct. Providers and the healthcare system are still on the front lines against COVID-19, and this rule establishes flexibilities for remote patient monitoring or other arrangements to assist in the ongoing response and recovery efforts."

Read on for details on the various impacts the updates have on health IT.

Understand the Stark EHR Exceptions

The Stark update follows through on many of CMS' 2019 proposals, offering a plethora of care coordination goodies that focus on giving patients more control of their healthcare decision-making.

Refresher: In a nutshell, Stark essentially was designed to prevent conflicts of interest. It bars physicians from referring Medicare or Medicaid beneficiaries to a designated health services (DHS) in which they or their family members have an ownership interest - unless, of course, an exception applies.

Stark is not a criminal statute, which means you won't go to jail if you break only this law. It's a civil statute enforced by CMS. If you violate Stark, you could face CMPs and exclusion from Medicare and other federal health programs.

IT exceptions: Due to overwhelming public commentary and recent 21st Century Cures Act developments, CMS updated its Stark-related EHR exceptions, expanding on current EHR donation rules and adding new cybersecurity exceptions. CMS decided two exceptions were better than one on this issue.

Here's why: The agency took commenters' worries seriously, and this impacted the decision. "We are finalizing our proposal to expand the EHR exception to expressly include cybersecurity software and services so that it is clear that an entity donating electronic health records 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 electronic health records, provided that all the requirements of the EHR exception are satisfied," the final rule explains.

Additionally, "CMS added protections for financial arrangements related to cybersecurity technology, to update and remove interoperability requirements and to remove the electronic health records exception's sunset date," note attorneys **Gretchen Heinze Townshend** and **Timothy J. Fry** with **McGuireWoods** in online analysis.

Review New and Modified Safe Harbors Under the AKS

OIG's final rule clarifies IT donations as one of its new safe harbors and also modifies a safe harbor related to EHRs.

AKS warning: Similar to Stark, the AKS covers referrals - and cautions about incentivizing them, especially for organizations that work in close quarters with different practitioners and labs who, naturally, refer to each other.

Under the AKS, "it is a felony to offer, provide, request, or accept any payment if one purpose is to influence payments under a federal healthcare program," reminds **David Glaser,** attorney with **Fredrikson & Byron, PA** in Minneapolis. "Paying referral sources is a big problem."

Unlike Stark, where your intent doesn't matter, an AKS violation would require improper intent, and AKS violations can garner both civil and criminal indictments. AKS "applies to any financial arrangements that impact federal healthcare program beneficiaries, e.g., TriCare and other programs in addition to Medicare and Medicaid," says attorney **Linda Baumann,** partner with **Arent Fox** in Washington, DC.

Safe harbors: OIG added a safe harbor for donations of cybersecurity technology and services, which is available to all types of individuals and entities," the final rule states.

"This safe harbor will protect arrangements intended to address the growing threat of cyber attacks impacting the healthcare ecosystem. In addition to software and other types of information technology, the final safe harbor will protect certain cybersecurity hardware donations that meet conditions in the safe harbor," OIG says.

Important: As part of the safe harbor, providers and entities will not be required to conduct a risk assessment before receiving donated hardware.

OIG modified its previous EHR safe harbor and beefed it up with added "protections for certain related cybersecurity technology, to update provisions regarding interoperability, and to remove the sunset date," a fact sheet indicates.

Start date: The changes in both final rules are effective Jan. 19, 2021.

Stay tuned for more analysis on the intersection of cybersecurity and enforcement in upcoming issues.

Resources: Review the Stark final rule at www.govinfo.gov/ content/pkg/FR-2020-12-02/pdf/2020-26140.pdf and peruse the AKS final rule at www.govinfo.gov/content/pkg/FR-2020- 12-02/pdf/2020-26072.pdf.