OIG ALERT

Office of Inspector General
330 Independence Ave., SW
Washington, DC 20201
Media: media@oig.hhs.gov
(202) 619-1343

For Immediate Release
October 6, 2015

OIG Policy Reminder:
Information Blocking and the Federal Anti-Kickback Statute

As the Department of Health and Human Services marks "National Health IT Week" 2015 and focuses on the flow of information across the care continuum, the Office of Inspector General (OIG) would like to take the opportunity to remind the public about how information blocking[1] may affect safe harbor protection under the Federal anti-kickback statute (42 U.S.C. 1320a-7b(b)).

About the Federal Anti-Kickback Statute:

The Federal anti-kickback statute prohibits individuals and entities from knowingly and willfully offering, paying, soliciting, or receiving remuneration to induce or reward referrals of business reimbursable under any Federal health care program (FHCP). Violation of the statute may also result in imposition of criminal penalties, civil monetary penalties, program exclusion, and liability under the False Claims Act (31 U.S.C. 3729–33). The types of remuneration covered specifically include, without limitation, kickbacks, bribes, and rebates, whether made directly or indirectly, overtly or covertly, in cash or in kind. The statute covers not only referrals of patients, but also the purchasing, leasing, or ordering of, or arranging for or recommending the purchasing, leasing, or ordering of, anything paid for by any FHCP.

There are, however, exceptions to the Federal anti-kickback statute, known as safe harbors. Health care providers, suppliers, and others may voluntarily seek to comply with a safe harbor to ensure that their payment or business practice will not be subject to sanctions under the Federal anti-kickback statute.

[1] The Office of the National Coordinator for Health IT has issued a Report to Congress on information blocking, which is available at http://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.

The Electronic Health Records Safe Harbor and Information Blocking:

In some cases, a provider, such as a hospital, may seek to furnish software or information technology to an existing or potential referral source, such as a physician practice. This kind of arrangement potentially implicates the Federal anti-kickback statute because the software or information technology is potential remuneration to the referral source. Arrangements involving the provision of software or information technology to a referral source should be scrutinized for compliance with the Federal anti-kickback statute. The electronic health records (EHR) safe harbor protects certain arrangements involving the provision of interoperable EHR software or information technology and training services. 42 CFR § 1001.952(y).[2] This safe harbor is intended "to protect beneficial arrangements that would eliminate perceived barriers to the adoption of EHR without creating undue risk that the arrangements might be used to induce or reward the generation of [FHCP] business." 71 FR 45111 (Aug. 8, 2006). OIG's goal is to "promot[e] the adoption of interoperable [EHR] technology that benefits patient care while reducing the likelihood that the safe harbor will be misused by donors to secure referrals." 78 FR 79208 (Dec. 27, 2013). The conditions included in the safe harbor help to strike that right balance. An arrangement must fit squarely in all safe harbor conditions to be protected.

One of the EHR safe harbor conditions is directly relevant to the issue of information blocking. That safe harbor condition requires that "[t]he donor (or any person on the donor's behalf) does not take any action to limit or restrict the use, compatibility, or interoperability of the items or services with other electronic prescribing or [EHR] systems (including, but not limited to, health information technology applications, products, or services)." 42 CFR § 1001.952(y)(3). In connection with this requirement, OIG has stated that "donations of items or services that have limited or restricted interoperability due to action taken by the donor or by any person on the donor's behalf (which could include the recipient acting on the donor's behalf) would fail to meet the condition at 42 CFR § 1001.952(y)(3) and is inconsistent with the intent of the safe harbor to promote the use of technology that is able to communicate with products from other vendors." 78 FR 79213 (Dec. 27, 2013). Failure to meet this condition would mean that the safe harbor would not apply and the arrangement would be subject to case-by-case review under the Federal anti-kickback statute. OIG has stated that such "donations would be suspect under the law as they would appear to be motivated, at least in part, by a purpose of securing [FHCP] business." Id.

A couple of examples illustrate this point. First, "arrangements in which a donor takes an action to limit the use, communication, or interoperability of donated items or services by entering into an agreement with a recipient to preclude or inhibit any competitor from interfacing with the donated system would not satisfy the requirement of 42 CFR § 1001.953(y)(3)." Id. Second, arrangements in which "[EHR] technology vendors agree with donors to charge high interface fees to non-recipient providers or suppliers or to competitors may also fail to satisfy the conditions of 42 CFR § 1001.952(y)(3)." Id.

[2] CMS has issued a corresponding exception to the physician self-referral law (42 U.S.C. 1395nn). See 71 FR 45140 (Aug. 8, 2006); 78 FR 78751 (Dec. 27, 2013). OIG coordinates closely with CMS concerning issues related to the EHR safe harbor and exception and have attempted to ensure as much consistency as possible between the two regulations, within the limitations imposed by the differences in the underlying statutes.

OIG continues to believe that "any action taken by a donor (or any person on behalf of the donor, including the [EHR] vendor or the recipient) to limit the use of the donated items or services by charging fees to deter non-recipient providers and suppliers and the donor's competitors from interfacing with the donated items or services would pose legitimate concerns that parties were improperly locking-in data and referrals and that the arrangement in question would not qualify for safe harbor protection." Id.

OIG notes that the EHR safe harbor contains additional conditions and limitations that must also be met for an arrangement to qualify for safe harbor protection. For example, the safe harbor requires that donated software be interoperable.[3] 42 CFR § 1001.952(y)(2). Further, the safe harbor offers protection only for donations from certain donors; laboratories are no longer potentially protected donors for purposes of the safe harbor. 42 CFR § 1001.952(y)(1).

Reporting Potentially Problematic Donation Arrangements:

OIG remains committed to investigating potentially abusive arrangements that purport to, but do not actually, meet the conditions of the EHR safe harbor. 78 FR 79213 (Dec. 27, 2013). OIG continues to encourage the public to report instances when a donor (or someone on their behalf) acts to limit the interoperability of donated items or services, because OIG believes that, when such lock-in has occurred, investigation may establish that safe harbor conditions have not been met. 78 FR 79215 (Dec. 27, 2013). Action taken to achieve that result could provide evidence of the intent to violate the Federal anti-kickback statute. Id. Those with information about arrangements that potentially violate the Federal anti-kickback statute are encouraged to contact OIG's hotline at 1–800–HHS–TIPS or visit https://forms.oig.hhs.gov/hotlineoperations/.

[3] For purposes of the EHR safe harbor, the term "interoperable" is defined in the Note to Paragraph (y). Software that, on the date it is provided to the recipient, has been "certified by a certifying body authorized by [ONC] to an edition of the [EHR] certification criteria identified in the then-applicable version of 45 CFR part 170" is deemed to be interoperable. 42 CFR § 1001.952(y)(2).