akerman

Blog Post

OIG Issues Information Blocking Penalties Final Rule: Health IT Developers and Health Information Exchanges/Networks Have a Million Reasons to Care

July 18, 2023

By Jordan T. Cohen, Noam B. Fischman, and Elizabeth F. Hodge

On June 27, 2023, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) issued its long-anticipated final rule amending the OIG's civil monetary penalty (CMP) regulations as they relate to information blocking (CMP Final Rule or Rule). The CMP Final Rule was published in the Federal Register on July 3, 2023. The Rule applies to entities that develop or offer certified health IT (collectively, Developers) and health information networks and health information exchanges (collectively, HIN/HIEs). Those subject to the CMP Final Rule should consider prioritizing their compliance efforts because the OIG will begin enforcing the Rule on September 1, 2023. Below we discuss the applicability of the CMP Final Rule, the assessment of penalties under the Rule, and the OIG's enforcement priorities moving forward.

Information Blocking Background

In 2016, the 21st Century Cures Act (Cures Act) made sharing electronic health information (EHI) the new normal in healthcare, with the twin goals of encouraging and incentivizing the free flow of patient information among stakeholders and driving efficiencies in healthcare. The Cures Act authorized

Related People

Jordan T. Cohen
Noam B. Fischman
Elizabeth F. Hodge

Related Work

Healthcare
Healthcare Fraud and Abuse
Healthcare Legislation and Government Affairs

Related Offices

New York
Washington, D.C.
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

the Secretary of HHS to identify "reasonable and necessary activities that do not constitute information blocking."[1] The Cures Act defined conduct that constitutes "information blocking," i.e., a practice by an "actor" that, except as required by law or specified in an information blocking exception, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.[2]

The information blocking provisions of the Cures Act apply to three categories of actors: healthcare providers, Developers, and HIN/HIEs. The Cures Act authorized the OIG to investigate claims of information blocking and provided the Secretary of HHS with authority to impose CMPs against Developers and HIN/HIEs for information blocking. The Cures Act also provides that any healthcare providers that the OIG determines have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives that HHS sets forth through notice and comment rulemaking.

In May 2020, the Office of the National Coordinator for Health Information Technology (ONC) published the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (ONC Final Rule or IB Rule). The IB Rule, among other things, promulgated regulations further defining what information blocking is and establishing reasonable and necessary activities that do not constitute information blocking, i.e., exceptions to the definition of information blocking.

On April 18, 2023, ONC published a proposed rule titled Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Proposed Rule(HTI-1 Proposed Rule), that would, among other things, update the IB Rule by revising the definition of information blocking and the manner and infeasibility exceptions.[3]

Final Rule Highlights

The CMP Final Rule authorizes the OIG to impose CMPs against Developers and HIN/HIEs who commit information blocking with penalties of up to $1 million per violation. Rather than creating a new CMP framework, the OIG is adding the CMP for information blocking to its existing Civil Monetary Penalties Law (CMPL) regulations and will apply the existing CMP procedural and appeal rights to complaints of information blocking. In the preamble to the CMP Final Rule, the OIG notes that information blocking "poses a threat to patient safety and undermines efforts by providers, payers, and others to make the health system more efficient and effective" and "may also constitute an element of a fraud scheme, such as by forcing unnecessary tests or conditioning information exchange on referrals." The CMP Final Rule also addresses enforcement and CMPs for fraud, false claims, or similar conduct in HHS grants, contracts, and other agreements, which are not addressed in this article.

Who: Applicability of CMPs for Information Blocking

The CMP Final Rule applies to two of three categories of "actors" under the Cures Act: Developers and HIN/HIEs who engage in a practice that, except as required by law or specified in an IB Rule exception, is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. The CMP Final Rule does not apply to healthcare providers unless they also fit the definition of Developers or HIN/HIEs. However, healthcare providers should note that HHS is developing a separate proposed rule, anticipated to be published in the fall of 2023, that will provide disincentives to healthcare providers who engage in information blocking.

How: How the OIG Will Assess CMPs for Information Blocking

As noted above, the OIG will follow its existing CMPL regulations when investigating complaints of information blocking by Developers or HIN/HIEs. This will entail making fact-specific determinations of whether the individual or entity meets the definition of a Developer or HIN/HIE and whether the alleged conduct meets ONC's definition of information blocking. The OIG anticipates working closely with ONC to make these threshold assessments. If the OIG determines that a Developer or HIN/HIE has engaged in information blocking, it will provide informal notice to the Developer or HIN/HIE and possibly engage in settlement negotiations. If the parties cannot reach a settlement, the OIG would then provide notice of the penalties to the actor consistent with 42 C.F.R. § 1003.1500. Developers and HIN/HIEs have the right to appeal the OIG's determination to the HHS Departmental Appeals Board consistent with 42 C.F.R. § 1005.2.

In the CMP Final Rule, the OIG explained its goal that the CMP be "fair, reasonable, and commensurate with the conduct so that wrongdoers are held accountable and future information blocking conduct is deterred." As a result, the OIG will use a fact-specific approach to assessing penalties — including consideration of aggravating and mitigating factors — instead of a one-size-fits-all formula or threshold.

Aggravating and Mitigating Factors. The OIG notes in the preamble that information blocking is novel and that it has limited experience in this area, and, as a result, it is only adopting the aggravating and mitigating factors set forth in the Cures Act. These statutory factors, which are now part of the CMP Final Rule, require the OIG to consider the nature and extent of the information blocking, as well as the harm resulting from the information blocking, including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted.

In refusing various commenters' requests for additional aggravating and mitigating factors, the OIG noted that it is required under the CMPL to consider certain general factors, including the nature of the claims and the circumstances in which they are presented; the degree of culpability, history of prior offenses, and financial condition of the person presenting the claims; and such other matters as justice may require. *See* 42 U.S.C. § 1320a–7a(d).

The OIG left open the possibility of implementing additional, specific factors in the future via notice and comment rulemaking as it gains more experience in enforcing the CMP for information blocking.

What is a Violation? A "violation" is a practice that constitutes information blocking as defined in the IB Rule. The OIG emphasizes in the Final Rule that "information blocking only requires engaging in a practice that is likely to interfere with, prohibit, or materially discourage the access, exchange, or use of EHI. Information blocking does not require that the practice actually interferes with, prohibits, or materially discourages the access, exchange, or use of EHI." The OIG expects that the maximum $1 million per violation penalty would apply to particularly egregious conduct. It declined to adopt specific criteria that it would use to identify single or multiple violations because it does not have enough information or experience with information blocking enforcement to establish uniform criteria. However, in response to certain hypotheticals, the OIG appears to have treated each impermissibly denied request as its own violation. Readers are encouraged to review pages 42830-42832 of the CMP Final Rule for the OIG's discussion of various hypotheticals.

Self-Disclosure Protocol to Come Later. The OIG noted that self-disclosure is a mitigating circumstance under the general factors. *See* 42 C.F.R. § 1003.140(a)(2). Relevant corrective action must include disclosing the violation to the OIG through

the self-disclosure protocol (SDP) and fully cooperating with the OIG's review and resolution of such disclosure. However, the OIG acknowledged that it does not currently have an SDP for information blocking and plans to create a specific SDP for information blocking after publication of the CMP Final Rule. The SDP will provide actors with a framework and mechanism for evaluating, disclosing, coordinating, and resolving CMP liability for conduct that constitutes information blocking. In the commentary to the Final Rule, the OIG stated that it will not develop an advisory opinion process regarding activities that may constitute information blocking because it lacks the statutory authority to do so.

OIG's Enforcement Priorities

The OIG expects to receive more information blocking complaints than it can feasibly investigate. To prepare for the predicted deluge, the OIG has explained that it will prioritize investigating and assessing penalties for information blocking practices that:

- result in, cause, or had the potential to cause patient harm, which is not restricted to individual harm, but rather may broadly encompass harm to a patient population, community, or the public;
- significantly impact a provider's ability to care for patients;
- occurred over an extended period of time;
- caused financial loss to federal healthcare programs or other government or private entities; or
- were performed with actual knowledge.

The OIG also notes that it may evaluate allegations and prioritize investigations based, in part, on the volume of claims relating to the same (or similar) conduct by the same actor. That evaluation would include assessment of all information blocking claims received by ONC from the public. The OIG

acknowledges that its enforcement priorities may evolve over time as it gains experience investigating information blocking complaints.

The OIG plans to partner with the ONC and other agencies as appropriate to review allegations. This partnership will involve, among other things, referring violations to other agencies for other regulatory considerations, such as the HHS Office for Civil Rights, the Federal Trade Commission, the Centers for Medicare and Medicaid Services, or the Department of Justice. Current anticipated enforcement priorities may therefore lead to investigations of HIPAA violations, anticompetitive conduct or unreasonable business practices, and False Claims Act violations, or possibly even criminal prosecution.

FCA Liability

Commenters to the CMP proposed rule asked about the potential for the OIG to use alternative mechanisms to enforce data blocking rules, including, among other possibilities, the potential for liability under the False Claims Act (FCA). In the Final Rule, the OIG hedged by stating that "[a]t this point, we do not anticipate using alternatives to CMPs as described by the commenters." Nevertheless, in different parts of the Final Rule, the OIG emphasized that it plans to work with other federal agencies in fashioning what it deems to be a comprehensive remedy for alleged violations of the IB Rule.

What would such collaboration look like? As context, between 2015 and 2022, the DOJ reported FCA settlements with health IT vendors in an amount exceeding $500 million. Those cases predominantly reflect enhanced DOJ efforts to enforce FCA liability in the kickback and false certification contexts. Health IT vendors should consider information blocking to be a new frontier of fraud and abuse enforcement. Compliance programs should be created (or adjusted) to account for ways in which

vendors certify compliance with federal rules and regulations (which now include information blocking initiatives). And compliance managers should adjust compliance plans to ensure that documentation reflects a current subjective intent to comply with those rules. Consistent with the Supreme Court's recent decision in *Supervalu*, courts will no longer credit an objectively reasonable interpretation of a rule or regulation as a defense to a FCA matter if the documentation does not support a party's subjective intent to comply with that rule or regulation. The mandate to avoid information blocking likely will become the first new set of rules and regulations through which the DOJ will test the breadth and depth of the *Supervalu* impact on a new set of FCA cases.

Next Steps:

- Those entities engaged in developing or offering certified health IT and HIN/HIEs should assess whether they may be subject to the ONC Information Blocking Rule and the OIG CMP Final Rule. While healthcare providers generally are not subject to the CMP Final Rule, they may be to the extent they also meet the definition of a Developer or HIN/HIE.
- For Developers and HIN/HIEs to whom this CMP Final Rule applies, minimizing exposure to potential information blocking violations is paramount. Developers and HIN/HIEs should ensure they have policies and procedures in place to comply with the Information Blocking Rule, including documenting those exceptions in the IBR upon which they rely to deny or delay the sharing of EHI.
- Healthcare providers should stay tuned for a separate proposed rule regarding appropriate disincentives for providers who engage in information blocking, which is expected in Fall 2023.
- Healthcare IT providers should calibrate compliance programs to ensure that they reflect a

subjective intent to comply with the new information blocking rules and review certifications to ensure that they fairly and accurately reflect current business practices.

- The April 2023 HTI-1 Proposed Rule demonstrates that the regulation of information blocking is evolving. Developers, HIN/HIEs, and healthcare providers should continue to monitor ONC's information blocking rulemaking activities because the CMP Final Rule relies heavily on the definitions in the ONC Information Blocking Rule.

Akerman's Health Law Rx blog will continue to monitor developments related to the CMP Final Rule and the anticipated proposed rule providing disincentives to healthcare providers who engage in information blocking.

*The authors would like to thank summer associate **Ameer Al-Khudari** for his assistance with this article.*

---

[1] https://www.healthit.gov/topic/information-blocking

[2] *Id.*; *see also* 42 U.S.C. § 3022(a)(1) (PHSA).

[3] *See* 74 Fed. Reg. 23746 (Apr. 18, 2023).
