ROPES & GRAY

ALERT

July 11, 2023

Renewed Focus on Information Sharing as OIG Finalizes Penalties of up to $1 Million per Information Blocking Violation

Attorneys
Christine Moundas
Gideon Zvi Palte
Carolyn Lye

On July 3, 2023, the long-awaited final rule from the U.S. Department of Health and Human Services ("HHS") Office of Inspector General ("OIG") titled "Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules" (the "OIG Final Rule") was published in the *Federal Register*.[1] The OIG Final Rule establishes civil monetary penalties ("CMPs") of up to $1 million per information blocking violation pursuant to Section 4004 of the 21st Century Cures Act (the "Cures Act").[2] Penalties may be imposed on developers of certified health information technology ("health IT") (including entities that offer certified health IT), health information exchanges ("HIEs"), and health information networks ("HINs") beginning on September 1, 2023. The OIG Final Rule concludes the rulemaking process that OIG began with a proposed rule published in the *Federal Register* on April 24, 2020 (the "OIG Proposed Rule") but does not establish information blocking penalties for health care providers, who will be subject "appropriate disincentives" to be established in future HHS rulemaking.

The OIG Final Rule provides helpful information to the industry regarding information blocking enforcement priorities, factors that will be considered in determining CMP amounts, and how OIG will coordinate with other agencies—such as the Office of the National Coordinator for Health IT ("ONC"), HHS Office for Civil Rights ("OCR"), Federal Trade Commission ("FTC"), Centers for Medicare & Medicaid Services ("CMS"), and Department of Justice ("DOJ")—on sanctions for information blocking violations. This information is important for developers of certified health IT, HIEs, HINs, and health care providers (collectively, "Actors") subject to information blocking to get a better sense of information blocking risk factors and the full scope of potential consequences for information blocking violations.

I. Information Blocking Background

Information blocking is defined in federal regulations issued by ONC as a practice that, except as required by law or covered by an information blocking exception, is likely to interfere with access, exchange, or use of electronic health information ("EHI"), and,

1. if conducted by a developer of certified health IT, HIE, or HIN, such Actor knows, or should know, that such practice is likely to interfere with access, exchange, or use of EHI; or

2. if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with access, exchange, or use of EHI.[3]

EHI is defined as electronic protected health information under the Health Insurance Portability and Accountability Act ("HIPAA") to the extent that it would be included in a designated record set as defined by HIPAA, regardless of whether the group of records are used or maintained by or for a covered entity under HIPAA. However, EHI does not include psychotherapy notes (as defined by HIPAA) or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[4] ONC's regulations also define information blocking "exceptions" that protect certain "reasonable and necessary activities" in which Actors may engage.[5] ONC recently proposed changes to its information blocking regulations, as we previously summarized here.[6]

ONC has provided several examples of activities that may be considered information blocking, including the following:

- A provider notifies its electronic health records software ("EHR") developer of its intent to switch to another EHR system and requests a complete export of its EHI. The developer will provide only the EHI in a PDF format, even though it already can and does produce the data in a commercially reasonable structured format.

- An EHR developer requires third-party applications to be "vetted" for security before use but does not promptly conduct the vetting or conducts the vetting in a discriminatory or exclusionary manner.

- An EHR developer maintains an "app store" through which other developers can have "apps" listed that run natively on the EHR developer's platform. The EHR developer charges app developers a substantial fee for this service unless an app developer agrees not to deploy the app in any other EHR developers' app stores.

- A developer of certified health IT takes significantly longer to provide or update interfaces that facilitate the exchange of EHI with users of competing technologies or services.

- A HIN's participation agreement prohibits entities that receive EHI through the HIN from transmitting that EHI to entities who are not participants of the HIN.

- Although not required by applicable law, a health care provider establishes an organizational policy that imposes delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results.

- Although an EHR developer's patient portal offers the capability for patients to directly transmit or request for direct transmission of their EHI to a third party, the developer's customers (e.g., health care providers) choose not to enable this capability.

- A health system incorrectly claims that the HIPAA Rules or other legal requirements preclude it from exchanging EHI with unaffiliated providers.

- A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider, but takes several days to respond.

- A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians that do not comply.[7]

II. OIG Final Rule

While ONC's information blocking regulations were finalized in 2020 and took effect on April 5, 2021, OIG did not finalize the 2020 OIG Proposed Rule until after the conclusion of the COVID-19 Public Health Emergency. Despite the long delay, the OIG Final Rule suggests that information blocking enforcement remains a priority for the government as it continues to promote interoperability and information sharing in the health care industry.

a. OIG Information Blocking Investigative Authority

Section 4004 of the Cures Act authorizes OIG to investigate any claims of information blocking by an Actor as well as to investigate claims that developers of certified health IT have submitted false attestations as part of the ONC Health IT Certification Program.[8] The Cures Act further authorizes the Secretary of HHS to impose a CMP of no more than $1 million per violation following a determination by OIG that a developer of certified health IT, HIE, or HIN has engaged in information blocking.[9] The Cures Act requires information blocking CMPs to be imposed within six years from the date the information blocking occurred.[10] The OIG Final Rule does not address potential information blocking violations by health care providers, who are not subject to CMPs under the Cures Act and who instead may be referred to the "appropriate agency to be subject to appropriate disincentives" to be specified in future HHS rulemaking.[111] However, OIG cautions that health care providers that also meet the definition of a developer, HIE, or HIN under ONC's regulations could be subject to CMPs. Therefore, it is important for health care providers to determine whether they may also be considered a different type of Actor that is subject to CMP liability.

b. Enforcement Priorities

OIG explains that it will prioritize investigating alleged conduct that "(1) resulted in, is causing, or had the potential to cause patient harm; (2) significantly impacted a provider's ability to care for patients; (3) was of long duration; (4) caused financial loss to Federal health care programs, or other government or private entities; or (5) was performed with actual knowledge."[12] Each allegation will be assessed individually to "determine whether it implicates one or more of the enforcement priorities, or otherwise merits further investigation and potential enforcement action."[13] If several allegations relating to the same or similar conduct by the same Actor are received, then OIG has indicated that it may prioritize investigations of all such allegations even if the individual allegations by themselves would not implicate any of OIG's specified priorities.

c. Determination of CMP Amounts

The Cures Act authorizes OIG to impose CMPs of up to $1 million per information blocking violation, which the OIG Final Rule explains would be appropriate for "particularly egregious conduct."[14] While OIG does not specify a CMP baseline or CMP thresholds, it provides some guidance regarding how the agency will determine the appropriate CMP amount in a particular case. CMP determinations may be appealed before an administrative law judge.[15]

i. Definition of "Violation"

The OIG Final Rule provides that OIG will impose a CMP for an information blocking "violation" and defines "violation" as "a practice, as defined in 45 CFR 171.102, that constitutes information blocking, as set forth in 45 CFR part 171."[16] OIG explains that if a single action preventing access to EHI affects multiple patients, then this action would constitute a single violation, although the number of patients affected would be considered in determining the penalty amount. On the other hand, if an Actor takes separate actions to deny requests for EHI because it has not implemented a system to deny all similar requests, OIG would consider each action to be a separate violation. Furthermore, OIG explains that adopting a policy or contractual provision that would result in information blocking would be considered a single violation, and each subsequent enforcement of the policy or provision would constitute an additional, separate violation.

ii. Analysis Factors

Under the Cures Act, determinations of the amount of CMPs to impose on entities found to have engaged in information blocking "must take into account factors such as the nature and extent of the information blocking and harm resulting from such information blocking, including, where applicable, the number of patients affected, the number of providers affected, and the number of days the information blocking persisted."[17] The OIG Final Rule implements these same statutory factors, with the clarification that the number of patients affected, the number of providers affected, and the number of days the information blocking persisted must all be considered for *both* the nature and extent of information blocking *and* the physical and financial harm that resulted from such information blocking.

In addition, OIG explains that the general factors that exist under the Civil Monetary Penalties Law apply in determining CMPs for information blocking. These include "(1) the nature of claims and the circumstances under which they were presented, (2) the degree of culpability, history of prior offenses, and financial condition of the person presenting the claims, and (3) such other matters as justice may require."[18] Additional considerations specific to alleged information blocking claims include whether an alleged information blocking violation actually interfered with access, exchange, or use of EHI; the number of violations; whether an Actor took corrective action; whether an Actor faced systemic barriers to interoperability; to what extent the Actor had control over the EHI; the Actor's size and market share; and whether the Actor had actual knowledge or specific intent to engage in information blocking.[19] OIG states that it may consider implementing additional factors for determining CMP amounts in future rulemaking after gaining more information blocking enforcement experience.

d. OIG Investigation Process and Coordination with Other Agencies

Throughout the OIG Final Rule, OIG emphasizes that it will coordinate with other agencies in connection with its information blocking investigation and enforcement efforts. These agencies may impose penalties for information blocking violations that supplement CMPs imposed by OIG. Agencies that OIG mentions include the following:

ONC: OIG explains that it "expect[s] that nearly all information blocking investigations will be done in coordination with ONC."[20] Both OIG and ONC will maintain mechanisms for reporting information blocking complaints,[21] and OIG assures stakeholders that the two agencies will coordinate closely regardless of which entity receives the complaint.[22] ONC may suspend or ban developers from the ONC Health IT Certification Program.

OCR: The Cures Act permits OIG to refer an information blocking complaint to OCR if the complaint involves conduct that may violate HIPAA.[23] For example, complaints involving interferences with individuals' access, exchange, or use of their own EHI may implicate both information blocking and the HIPAA right of access.[24] HIPAA violations may lead to civil litigation and monetary penalties and, in some cases, criminal liability.

FTC: Similarly, the Cures Act permits OIG to share information with FTC for complaints that may involve unfair trade practices and anticompetitive conduct,[25] and OIG plans to work with ONC to identify allegations that warrant referral to FTC.[26] FTC may impose civil penalties for unfair trade practices and anticompetitive conduct under the FTC Act.

CMS: OIG explains that it may refer to CMS complaints involving potential noncompliance with CMS programmatic requirements, such as noncompliance relating to the Merit-Based Incentive Payment System ("MIPS") or admission, discharge, and transfer notifications required for certain hospitals participating in Medicare.[27] CMS may impose penalties in connection with Medicare program participation, such as requiring corrective action plans to remedy deficiencies or terminating Medicare program participation.

DOJ: OIG warns that information blocking violations could create False Claims Act ("FCA") liability for an Actor and that it will coordinate with DOJ in such cases. To explain how an information blocking violation could implicate the FCA, OIG provides an example of a developer that falsifies information provided to ONC as part of the ONC Health IT Certification Program. OIG explains that such false attestations may cause health care providers to file false attestations under MIPS.[28] In this example, it is possible that both the health care provider and the developer could be regarded as violating the law—the health care provider for submitting a claim based on false attestations and the developer for causing the submission of such false claims by causing the provider's attestations to be false. FCA violations may lead to liability of up to triple the amount paid from the false claims, as well as CMPs. Potential FCA liability in OIG's example could be significant and could provide a large incentive for *qui tam* relators, who may share in FCA recoveries by the government, to bring FCA claims predicated on information blocking violations.

e. Self-Disclosure Process

OIG intends to create an information blocking self-disclosure process ("SDP") to allow Actors to self-disclose potential information blocking violations to OIG and for OIG to evaluate, coordinate, and resolve CMP liability for conduct that constitutes information blocking. OIG has also established SDPs for health care fraud violations by providers, HHS contractors, and HHS grant recipients,[29] and CMS has an SDP for Stark Law violations.[30] OIG's establishment of an information blocking SDP could suggest that OIG anticipates actively investigating and imposing CMPs for information blocking violations. While SDP self-disclosure may reduce the amount of potential CMPs, it will not absolve an Actor from liability for other potential consequences of information blocking violations.[31] For example, a developer that self-discloses information blocking through the SDP could still be subject to ONC enforcement, including termination of health IT certification for its products as well as fines and penalties from OCR for practices involving violations of HIPAA requirements. Actors should carefully consider the risks of non-CMP liability against the potential benefits of self-disclosing information blocking violations to OIG, particularly given that OIG will coordinate closely with other agencies in information blocking investigations.

III. Conclusion

Despite the long delay between the release of the OIG Proposed Rule and the publication of the OIG Final Rule, OIG now appears to be focused on investigating claims of information blocking. OIG information blocking enforcement is significant because it introduces sanctions for information blocking violations by HIEs and HINs and raises the stakes of information blocking violations by developers, who now may be subject to CMPs in addition to being banned or suspended from the ONC Health IT Certification Program. While the OIG Final Rule provides some helpful information regarding how OIG will investigate and penalize information blocking violations, it also suggests that such violations may involve liability

imposed by other agencies on top of potentially significant OIG-imposed CMPs. In addition, both OIG and ONC will provide mechanisms for anyone to report potential information blocking violations either online or by telephone, and the OIG Final Rule's discussion of potential FCA liability may inspire *qui tam* actions alleging FCA liability predicated on information blocking violations. To mitigate risk, Actors should review their EHI-related practices to identify and remediate any conduct that could be considered information blocking.

If you have any questions regarding the OIG Final Rule, please do not hesitate to contact one of the authors or your regular Ropes & Gray advisor.

1. 88 Fed. Reg. 42,820 (July 3, 2023).
2. 42 U.S.C. § 300jj–52. The OIG Final Rule also incorporates new authorities for CMPs, assessments, and exclusions related to HHS grants, contracts, and other agreements and increases the maximum penalties for certain CMP violations.
3. 45 C.F.R. § 171.103.
4. 45 C.F.R. § 171.102. Prior to October 6, 2022, EHI was limited to information identified by the data elements represented in the United States Core Data for Interoperability version 1 standard.
5. 45 C.F.R. Part 171, Subparts B and C; issued pursuant to 42 U.S.C. § 300jj–52(a)(3).
6. *See* Christine Moundas, Gideon Zvi Palte, and Carolyn Lye, "ONC Proposes Significant Changes to Health IT Certification Program and Information Blocking Rule," Ropes & Gray LLP (April 21, 2023).
7. For additional examples, *see* ONC, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule, 84 Fed. Reg. 7424, 7518–21 (March 4, 2019); ONC, *Information Blocking Frequently Asked Questions*, (last visited July 5, 2023).
8. 42 U.S.C. § 300jj–52(b)(1)(A).
9. 42 U.S.C. § 300jj–52(b)(2)(A). Separately, Section 4002 of the Cures Act (42 U.S.C. § 300jj–11) requires ONC to establish a prohibition on information blocking as a required condition for obtaining and maintaining health IT certification. ONC has codified this requirement in federal regulations at 45 C.F.R. § 170.401.
10. *See* 88 Fed. Reg. at 42,826.
11. 42 U.S.C. § 300j–52(b)(2)(B).
12. *See* 88 Fed. Reg. at 42,822.
13. *See* 88 Fed. Reg. at 42,823.
14. *See* 88 Fed. Reg. at 42,834.
15. *See* 88 Fed. Reg. at 42,826.
16. 42 C.F.R. § 1003.1410(a).
17. 42 U.S.C. § 300jj–52(b)(2)(A).
18. 42 U.S.C. § 1320a–7a(d).
19. *See* 88 Fed. Reg. at 42,833.
20. *See* 88 Fed. Reg. at 42,826.
21. Claims of information blocking can be submitted to OIG online at https://tips.oig.hhs.gov/ or by phone at 1-800-447-8477. *See* 88 Fed. Reg. at 42,823. In addition, complaints can be submitted through ONC's information blocking online portal. *See* ONC, *Information Blocking Portal*, (last visited June 29, 2023).
22. *See* 88 Fed. Reg. at 42,823.
23. 42 U.S.C. § 300jj–52(b)(3)(A).
24. 45 C.F.R. § 164.524.
25. 42 U.S.C. § 300jj–52(d)(1).
26. *See* 88 Fed. Reg. at 42,824.
27. *See* 42 C.F.R. §§ 482.24(d) (hospitals), 482.61(f) (psychiatric hospitals), and 485.638(d) (critical access hospitals).
28. *See* 88 Fed. Reg. at 42,824.
29. *See* OIG, *Self-Disclosure Information*, (last visited June 29, 2023).
30. *See* CMS, *Self-Referral Disclosure Protocol*, (last updated March 1, 2023).
31. *See* 88 Fed. Reg. at 42,825.