SPECIAL REPORT

A Million Reasons to Share: OIG's Final Rule on Information Blocking Enforcement

JULY 7, 2023

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

JAMES CANNATTI
PARTNER

jcannatti@mwe.com
Tel +1 202 756 8866

DANIEL GOTTLIEB
PARTNER

dgottlieb@mwe.com
Tel +1 312 984 6471

ALYA SULAIMAN
PARTNER

asulaiman@mwe.com
Tel +1 310 788 6017

SCOTT WEINSTEIN
PARTNER

sweinstein@mwe.com
Tel +1 202 756 8671

For more information about McDermott Will & Emery visit mwe.com

INTRODUCTION

On July 3, 2023, the US Department of Health and Human Services (HHS) Office of Inspector General (OIG) published its final rule (OIG final rule) in the *Federal Register* amending its existing civil monetary penalty (CMP) law (CMPL) regulations. The amendments implement OIG's authority under the 21st Century Cures Act (Cures Act) to investigate claims of information blocking and assess CMPs of up to $1 million—inflation adjusted to $1,162,924, currently—for information blocking violations by a health IT developer of certified health IT (certified health IT developer) or a health information network or health information exchange (HIN/HIE).

The OIG final rule does not apply to health care providers except to the extent they meet the definitions of a certified health IT developer or HIN/HIE. However, a separate rule will implement the Cures Act provision authorizing "appropriate disincentives" against healthcare providers that have committed information blocking. As noted in the OIG final rule, HHS is actively drafting a proposed rule to establish what the HHS Unified Agenda refers to as the "first set" of appropriate disincentives.

Under the OIG final rule, the information blocking regulations adopted by the HHS Office of the National Coordinator for Health Information Technology (ONC) under the Cures Act are incorporated into OIG's CMP regulations as the basis for determining whether information blocking occurred. Under the ONC's regulations, a certified health IT developer or HIN/HIE (collectively, actors) engages in information blocking if it knows, or should know, that its practice is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information (EHI), unless the practice is required by law or meets one of the eight exceptions in ONC's regulations. OIG emphasized throughout the final rule that it will rely on ONC's technical expertise and coordinate its review of allegations of information blocking and enforcement activities closely with ONC and other relevant federal agencies (*e.g.*, the HHS Office for Civil Rights).

In this *Special Report*, we discuss key takeaways from the OIG final rule, including information blocking reporting, investigation and enforcement procedures, and recommended action items.

For information about ONC's information blocking regulations, including who is a regulated actor, as well as important information blocking definitions and exceptions, see our *Special Report*. For information about OIG's proposed rule to implement its CMP authority, see our earlier *On the Subject*.

ENFORCEMENT TIMING

Consistent with OIG's statements in its proposed rule, OIG will not begin enforcement until 60 days after publication of the OIG final rule in the *Federal Register*—making the effective date of the OIG final rule September 1, 2023. Importantly for certified health IT developers and HIN/HIEs, OIG will not impose a CMP for any information blocking conduct occurring before OIG's effective date. However, in a recent presentation at the American Health Law Association Annual Meeting, OIG representatives stated that conduct occurring before the OIG final rule's effective date might be taken into account if a claim relates to the same or similar conduct by an actor over time.

DEFINITION OF AN INFORMATION BLOCKING VIOLATION

OIG adopted a very broad definition of a "violation" in the OIG final rule, stating that a violation is a practice that constitutes information blocking as set forth in ONC's information blocking regulations. This is particularly important because CMPs and the $1 million cap on penalties are established on a per-violation basis. In addition, OIG reminds readers that information blocking can involve conduct that is related to technologies certified under ONC's regulatory framework *or* non-certified health information technology.

The OIG final rule includes a few helpful examples regarding when, according to OIG, certain conduct would constitute a single information blocking violation subject to the $1 million CMP cap or multiple violations subject to multiple CMPs.

Example 1: Denial of Single Request for Multiple Patients Records = Single Violation

OIG states that a certified health IT developer's denial of a single request by a health care provider to receive multiple patients' information via an application programming interface (API) would be a single information blocking violation even though the problematic conduct prevents access to multiple patients' EHI. OIG states that it would consider the number of patients affected by the violation when determining the amount of the CMP.

Example 2: Multiple Denials of Multiple Requests = Multiple Violations

On the other hand, in another example, OIG indicates that when a certified health IT developer takes multiple separate actions to improperly deny multiple individual requests by a healthcare provider for EHI through an API, OIG would consider each separate action to be a separate information blocking violation.

Example 3: Single System Update Resulting in Multiple Request Denials = Single Violation

A third example indicates that OIG would treat as a single violation a certified health IT developer's update to its system to deny all requests made by anyone using a particular third party's technology even if the system update resulted in the denial of multiple requests. Again, OIG may consider the number of patients affected by the system change to be an aggravating circumstance meriting an increased CMP amount.

OIG also notes that enactment of a policy that constitutes information blocking may be a single violation and each action taken to enforce that policy may be a separate, additional violation. A key takeaway from the examples in the final rule is that OIG is focused primarily on the number of deliberate actions taken by an actor that impact requests to access, exchange or use EHI.

OIG ENFORCEMENT PRIORITIES

OIG anticipates focusing enforcement based on the same enforcement priorities that it described in its preamble to its proposed rule in 2020.

In evaluating the priority related to patient harm, OIG clarifies that its focus is not specific to individual harm, but rather encompasses harm to a patient population, community or the public.

Information Blocking Enforcement Priorities

OIG will allocate resources and prioritize enforcement against actors that engage in information blocking violations that include any of the following factors:

1. Resulted in, is causing or had the potential to cause patient harm
2. Significantly impacted a healthcare provider's ability to care for patients
3. Was of long duration
4. Caused financial loss to Medicare, Medicaid or other federal healthcare programs or other government or private entities
5. Was performed with actual knowledge.

The "actual knowledge" priority factor is noteworthy because ONC's definition of information blocking includes practices that a certified health IT developer or HIN/HIE "knows" or "should know" are likely to interfere with the access, exchange or use of EHI. OIG explains that the conduct of someone acting with actual knowledge is generally more egregious than the conduct of someone who only *should know* that their practice is likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.

In addition to the five priority factors, OIG may evaluate allegations and prioritize investigations based on the volume of claims relating to the same (or similar) conduct by the same actor. Like other OIG authorities that include an intent element, OIG emphasizes that each information blocking allegation will require a facts and circumstances analysis, which OIG will conduct in coordination with ONC and other federal agencies, as appropriate. (See discussion below regarding OIG's anticipated coordination with other federal regulators.)

Note that while OIG's enforcement priorities may inform OIG's decisions about which allegations to investigate, OIG states that the priorities are *not* dispositive. OIG may reassess these priorities over time.

REPORTING VIOLATIONS

The Cures Act required ONC to implement a standardized process for the submission of reports on claims of information blocking and to share information with OIG. ONC has implemented that standardized process for the public to submit claims of information blocking through its website. In addition to the process required by the Cures Act, OIG stated that it will accept complaints of information blocking through its usual complaint hotline through its website or by phone. OIG states that it will coordinate with ONC in evaluating claims of information blocking and share information regardless of whether a claim is made to ONC or OIG.

Note that ONC publishes statistics about information blocking claims it has received through its "*Report Information Blocking Portal*" on its website and updates this information monthly. As of July 5, 2023, ONC reports that it has received 708 possible claims of information blocking.

SELF-DISCLOSURE PROTOCOL

OIG states that after the publication of its final rule, it will add an information blocking self-disclosure protocol (SDP) to OIG's existing SDP for actors seeking to resolve potential CMP liability for information blocking conduct and to allow for lower CMP amounts as part of the resolution. According to OIG, the information blocking SDP will provide actors with a framework and mechanism for evaluating, disclosing, coordinating and resolving CMP liability for conduct that constitutes information blocking. OIG states that it will accept self-disclosure of information blocking conduct even before it releases the information blocking-specific SDP.

OIG notes that there are "significant benefits" for actors that self-disclose potential information blocking. Actors that cooperate with OIG during the self-disclosure process are expected to pay lower CMP amounts than would normally be required in resolving an investigation initiated by OIG. In addition, OIG believes that self-disclosure provides the opportunity for an actor to avoid costs and disruptions associated with government-directed investigations and civil or administrative litigation. However, a self-disclosure would not resolve liability for potential violations under HIPAA or other laws and involves other risks that should be weighed carefully.

While an SDP pathway may be helpful in some instances, it is unfortunate that OIG concluded that it does not currently have the authority to issue advisory opinions concerning the information blocking

CMPs, like it does for so many of its other CMP authorities. That said, and while OIG doesn't currently plan to develop an advisory opinion process for information blocking CMPs, OIG does acknowledge that the Justification of Estimates to the Appropriations Committee for President Biden's FY 2024 budget includes a legislative proposal for providing HHS for such advisory opinion authority.

CMP PROCESS AND APPEAL RIGHTS

Consistent with its proposed rule, OIG added the CMP for information blocking to its existing CMPL regulations and applied the existing CMPL procedural and appeal rights to the CMP for information blocking.

OIG Investigation and Enforcement Process

According to OIG, the investigation and enforcement process is expected to include the following steps:

1. OIG receives an information blocking complaint.
2. OIG uses its enforcement priorities discussed above to assess the complaint.
3. OIG opens an information blocking case.
4. OIG investigates the complaint by gathering facts, conducting interviews, making document requests, etc., using its documentary and testimonial subpoena powers:
    a. OIG may consult with ONC to assess facts and information blocking regulations.
    b. OIG closes the case if OIG concludes information blocking was not committed.
5. If OIG does not close the case, then OIG provides an opportunity for the actor to discuss OIG's investigation.
6. If OIG concludes the entity committed information blocking, OIG sends a demand letter to the actor.
7. The actor has the opportunity to appeal OIG's imposition of a CMP.

OIG must initiate an action for CMPs within six years from the date the information blocking violation occurred. According to OIG, actors in a CMP enforcement action bear the burden of proof for affirmative defenses and mitigating circumstances by a preponderance of the evidence. Accordingly, actors should consider retaining, for at least six years from their creation, documents demonstrating compliance. This is particularly true to the extent an actor plans to rely on an information blocking exception under ONC's regulations that includes a documentation element.

FACTORS AFFECTING CMP AMOUNTS

OIG states that it aims for fair CMP amounts and intends to take into account the particular facts and circumstances of each violation and not follow "one-size-fits-all formulas or thresholds." Under the Cures Act, when assessing a CMP for information blocking, OIG must consider, among any other factors, 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. The final rule likewise requires OIG to consider these factors.

General Factors to Determine Civil Monetary Penalty Amounts

In addition, as required by the Cures Act, OIG will consider the pre-existing general factors under the CMPL regulations when determining CMP amounts, including the following:

- The nature and circumstances of the violation
- The degree of culpability (*e.g.*, knows or should know)
- History of prior offenses
- Use of self-disclosure protocol
- Other wrongful conduct
- Such other matters as justice may require.

OIG acknowledges that the general factors may overlap with the new factors under the Cures Act and it will take into account the similarity of factors to avoid a "double count."

When assessing the "nature and circumstances" under the general factors and "nature and extent" under the Cures Act factors, OIG notes that it may consider whether a practice actually interfered with the 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 the market share. As required by the Cures Act, OIG must consider the number of patients affected, number of providers affected and the duration of the information blocking conduct when considering the nature and extent and harm factors. OIG states that it may also consider the number of organizations impacted by the information blocking, in addition to the number of patients and providers affected.

To assess harm under the Cures Act factors, OIG intends to consider whether any physical, financial or other harm occurred and evaluate the severity and extent of the harm.

OIG also states that a self-disclosure of information blocking conduct may be a mitigating circumstance because taking appropriate and timely corrective action in response to a violation is a mitigating circumstance under the general CMPL regulations' degree of culpability factor.

Once OIG proposes a penalty amount, the actor may request that OIG consider its financial condition and ability to pay the proposed CMP amount.

COORDINATION WITH OTHER AGENCIES

As noted above, OIG expects ONC to serve as a technical consultant and intends to coordinate its enforcement activities closely with ONC. In addition, when evaluating claims, OIG anticipates referring matters to other federal agencies for potential enforcement under their respective authorities and to avoid duplicative penalties.

Under the Cures Act, OIG may request technical assistance from, or refer certain information blocking allegations to, OCR to address issues arising under the HIPAA Privacy and Security Rules. For example, OIG states that it may consider referring certain claims of alleged interference with patients' access to their medical records to OCR, which has brought numerous enforcement actions for alleged violations of the Privacy Rule's right to access.

In addition, OIG notes that allegations of information blocking may also identify potential false statements to ONC by certified health IT developers during the testing and certification process under the ONC Health IT Certification Program. Such conduct could be referred to ONC and/or the Department of Justice for, among other things, consideration of potential federal False Claims Act liability.

OIG also expects to coordinate with the Federal Trade Commission on information blocking claims that involve allegations of anti-competitive conduct or unreasonable business practices, such as unconscionable or one-sided business terms for the access, exchange or use of EHI, or the licensing of an interoperability element. OIG states that a contract containing unconscionable terms related to sharing of patient data could be anti-competitive conduct that impedes a provider's ability to care for patients.

RECOMMENDED ACTION ITEMS

Certified health IT developers, HIN/HIEs and healthcare providers that might meet these actor definitions based on their activities should consider the following actions before the OIG Final Rule goes into effect on September 1, 2023 (if not already completed):

- ✓ Take full advantage of the next two months to review policies, procedures and practices affecting access, exchange or use of EHI to confirm that they are consistent with ONC's information blocking regulations and related laws, such as HIPAA and ONC's Health IT Certification Program requirements.
- ✓ Review, update or create documentation describing your organization's commitment to health information sharing consistent with ONC's regulatory framework and policy initiatives.

- ✓ Train personnel responsible for negotiating and implementing collaborations, partnerships and other arrangements with third parties (*e.g.*, digital health companies and consumer-facing app developers) seeking access, exchange or use of EHI, to avoid conduct that may lead to information blocking claims.
- ✓ Train personnel responsible for implementing APIs, interfaces and other interoperability elements regarding interoperability expectations, requirements under the ONC's information blocking regulations and OIG's enforcement priorities.
- ✓ Refine processes to create and retain records and other documents demonstrating the organization's compliance with ONC's information blocking regulations, including relevant exceptions.
- ✓ Interview and identify defense counsel to help navigate a potential OIG investigation so the organization is prepared in the event of an actual investigation.
- ✓ Consider, for any problematic conduct that continues after the September 1, 2023, effective date, whether to self-disclose any information blocking conduct.

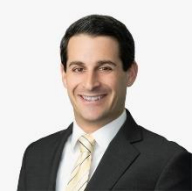
Please contact your regular McDermott lawyer or any of the authors of this *Special Report* if you have questions about the OIG final rule or if you need assistance with your compliance obligations under the ONC's information blocking regulations or responding to OIG inquiries. We are here to help.

CONTRIBUTORS

JAMES CANNATTI
PARTNER
jcannatti@mwe.com
Tel +1 202 756 8866

DANIEL GOTTLIEB
PARTNER
dgottlieb@mwe.com
Tel +1 312 984 6471

ALYA SULAIMAN
PARTNER
asulaiman@mwe.com
Tel +1 310 788 6017



SCOTT WEINSTEIN
PARTNER
sweinstein@mwe.com
Tel +1 202 756 8671

McDermott
Will & Emery

mwe.com |