

OIG Issues Final Information Blocking Enforcement Rule and Highlights the Potential for Referrals to the FTC and FCA Liability

Health Care Law Brief on July 25, 2023

On June 27, 2023, the Office of Inspector General (“[OIG](#)”) for the U.S. Department of Health and Human Services (“[HHS](#)”) [released](#) its final rule (“[Final Rule](#)”) implementing penalties for information blocking.

The Final Rule codifies the prohibition on “information blocking” introduced by the 21st Century Cures Act (“[Act](#)”), which was enacted on December 13, 2016. In the Act, “information blocking” was defined as any activity that, in part, is “likely to interfere with, prevent, or materially discourage access, exchange, or use” of electronic health information (“[EHI](#)”).^[1] The Final Rule provides an enforcement process for alleged information blocking violations by health information networks, health information exchanges, and developers of health IT certified by the HHS Office of the National Coordinator for Health Information Technology (“[ONC](#)”). Enforcement of the information blocking penalties will begin on September 1, sixty days after publication of the final rule in the [Federal Register](#).

OIG’s Stated Enforcement Priorities Indicate a Focus on Repeated or Egregious Conduct

In the preamble to the Final Rule, OIG described its enforcement priorities. “[T]o triage allegations and allocate resources,” OIG will prioritize and select cases for investigation where the alleged conduct:

- (i) resulted in, is causing, or had the potential to cause **patient harm**;
- (ii) significantly impacted a provider’s **ability to care for patients**;
- (iii) was of **long duration**;
- (iv) **caused financial loss** to Federal health care programs, or other government or private entities; or
- (v) was performed with **actual knowledge**.^[2]

In addition to these priorities, OIG also explained how 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.”[\[3\]](#) Given the foregoing statement, OIG enforcement actions, at least as a preliminary matter, are likely to focus on repeat offenders, or particularly flagrant conduct.

The Final Rule Includes Anti-Competitive Conduct as an Enforcement Priority and Highlights the Pathway for Referrals to FTC

In what can be characterized as a warning to developers, exchanges, and networks concerning their commercial contracting practices, OIG stated that its “current anticipated enforcement priorities may lead to investigations of anti-competitive conduct or unreasonable business practices.” Specifically, OIG signaled that “unconscionable or one-sided business terms for the access, exchange, or use of EHI, or the licensing of an interoperability element” may rise to the level of information blocking if the conduct “impedes a provider’s ability to care for patients.”[\[4\]](#)

OIG’s declaration indicates that it may, in part, focus its investigations on competition and private commercial activity, an area of inquiry typically within the purview of the Federal Trade Commission (“[FTC](#)”) and State Attorneys General. Alone, such declaration is unusual, given that investigations into unfair business practices, including anti-competitive practices, are beyond the purview of OIG. Unsurprisingly, the very next section of the Final Rule, concerning “Coordination with Other Agencies,” provides important additional context regarding the competition-related commentary. In that section, OIG highlights that the Act “includes specific options for ONC and OIG to coordinate with the FTC.”[\[5\]](#)

Rules Concerning Provider “Disincentives” are Forthcoming

Of note, the Final Rule does not apply to health care providers. Unlike developers, exchanges, and networks, the Act does not empower OIG to directly assess penalties for non-compliance against health care providers.[\[6\]](#) Instead, under the Act, health care providers “shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary sets forth through notice and comment rulemaking.”[\[7\]](#)

In developing such “disincentives,” HHS is likely to look at its existing authority to punish conduct that rises to the level of “information blocking” by health care providers, and may look to the authority granted to it under the Health Insurance Portability and Accountability Act and the regulations promulgated thereunder (“HIPAA”). For example, ONC’s information blocking [landing page for health care providers](#) contains references to a patient’s right of access under HIPAA, suggesting that HIPAA-related penalties will serve as the foundation for the forthcoming information blocking “disincentives.”

At [a recent health care conference](#), HHS officials stated that they anticipate the provider disincentive rules to be published this fall. Moreover, the officials described their active collaboration with HHS’s Office for Civil Rights (“OCR”), which is tasked with enforcing HIPAA.

Health Care Providers May Be Exposed to False Claims Act (“FCA”) Liability for Failures by Developers

Unsurprisingly, OIG provided limited commentary with respect to the FCA in the Final Rule—a statute not within OIG’s enforcement jurisdiction. Nevertheless, OIG described a novel theory of FCA liability. The agency stated that, “by engaging in conduct that constitutes information blocking, a health IT developer of certified health IT may have falsified attestations made to ONC as part of the ONC Health IT Certification Program,” which, in turn, may “cause health care providers to file false attestations under MIPS [Merit-based Incentive Payment System].”[\[8\]](#)

Although OIG offered no commentary as to whom may be liable for the filing of potentially false claims, the example it cited is illustrative: A developer’s failure to comply with information blocking regulation may ultimately result in the submission of false claims by a health care provider, if the provider participates in MIPS and attests to the use of certified health IT. In light of the foregoing commentary, novel FCA claims against health care providers, rooted in a developer’s violation of information blocking rules, cannot be ruled out.

Practical Implications

Developers, Networks and Exchanges

In the event that OIG determines that a developer, exchange, or network has engaged in “information blocking,” the agency may impose a civil monetary penalty (“CMP”) of up to \$1 million per violation.^[9] OIG intends to create a [self-disclosure protocol](#) which will provide a “framework and mechanism for evaluating, disclosing, coordinating, and resolving CMP liability for conduct that constitutes information blocking.”^[10] Although the protocol is not yet published, “OIG will accept self-disclosure[s] of information blocking conduct.”^[11] In discussing the benefits of self-disclosure in the Final Rule, the agency noted that “it is a mitigating circumstance under the factors at 42 CFR 1003.140(a)(2) for an actor to take appropriate and timely corrective action in response to a violation.”^[12]

Health Care Providers

At this time, the information blocking “disincentives” for health care providers remain forthcoming. However, health care providers may stand to benefit from the Final Rule, in that the Final Rule may discourage information blocking by developers and may spur the adoption of provider-friendly contract terms given that the Final Rule explicitly calls attention to “unconscionable or one-sided business terms for the access, exchange, or use of EHI.”

Nevertheless, the information blocking regulations and the Final Rule contribute to an ever-expanding regulatory burden for health care providers. For example, the Final Rule alludes to potential FCA liability where a health care provider participates in MIPS and utilizes certified health IT that fails to comply with the information blocking rules. Moreover, ONC’s efforts to solicit complaints regarding information blocking have largely resulted in complaints being lodged against health care providers. For example, between April 5, 2021 and May 31, 2023, ONC received 708 complaints alleging “possible claims of information blocking,” of which 598 (79%) were from patients or on a patient’s behalf, and in which health care providers were named as the alleged violating actors 80% of the time.^[13] ONC’s efforts to solicit public complaints, in addition to those efforts by OCR and state medical boards or related authorities, may result in a scenario in which aggrieved patients or their attorneys weaponize the complaint process to lodge burdensome complaints with ONC, OCR, and state medical boards or related authorities.

[1] See 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, (2016); 42 U.S.C. § 300jj-52(a); 45 C.F.R. § 171.103.

[2] See Final Rule, Section III.A, available at: <https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/infoblocking-rule-unofficial-hhs-oig.pdf>.

See also U.S. Department of Health and Human Services, Office of Inspector General, *Featured Topics: Information Blocking, Enforcement Priorities*, available at: <https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/>.

[3] Final Rule, Section III.A.

[4] Final Rule, Section III.A (citing to 85 FR 25812, May 1, 2020, available at: <https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification>).

[5] Final Rule, Section III.B. See also 42 U.S.C. § 300jj-52(d)(1) (setting forth that the “National Coordinator may, notwithstanding any other provision of law, share information related to claims or investigations under subsection (b) with the Federal Trade Commission for purposes of such investigations and shall share information with the Inspector General, as required by law”).

[6] 42 U.S.C. § 300jj-52(b)(2).

[7] 42 U.S.C. § 300jj-52(b)(2)(B).

[8] Final Rule, Section III.C.

[9] See Final Rule, Section IV.

[10] See Final Rule, Section III.C.

[11] *Id.*

[12] *Id.*

[13] U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, *Information Blocking Claims: By the Numbers*, available at: <https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers>. The ONC dataset concerning “claims count by potential actors” sets forth that the agency has received 598 claims naming health care providers, of 744 total listed on the chart.

Related Professionals

- **Jonian Rafti**
Associate