

Coppersmith Briefs

IBR Enforcement is Here:

What the Proposed HHS Disincentives Rule Means for Health Care Providers and the Final OIG CMP Rule Means for Health IT Developers and HIN/HIEs

Melissa A. Soliz and Benjamin Yeager, Coppersmith Brockelman PLC | December 5, 2023

INTRODUCTION

Since launching its complaint portal in April of 2021, the Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC) has received over 800 claims of possible information blocking with approximately 80% made against health care providers.¹ Despite these numbers, enforcement of the 21st Century Cures Act (Cures Act) Information Blocking Rule (IBR) has been delayed pending finalization of the enforcement rules. Those enforcement rules have been released. Specifically:

- The Office of the Inspector General (OIG) finalized the Civil Money Penalty (CMP) regulation (the “[OIG CMP Rule](#)”) on July 3, 2023, and started enforcement of the OIG CMP Rule against health information technology (IT) developers of certified health IT (“health IT developers”) and health information networks/exchanges (“HIN/HIEs”) on September 1, 2023. OIG will not impose CMPs for information blocking that occurred before that date.² Health IT developers and HIN/HIEs found by OIG to have committed information blocking face CMPs up to \$1 million per violation.
- On November 1, 2023, the Centers for Medicare & Medicaid Services (CMS) and the ONC proposed the HHS Disincentives regulation (the “[Proposed HHS Disincentives Rule](#)”),³ which would establish the enforcement structure for health care providers determined by OIG to have committed information blocking. Health care providers who commit information blocking face disincentives if they participate in the CMS Medicare Promoting Interoperability Program, the Medicare Merit-Based Incentive Payment System (MIPS) Promoting Interoperability performance category, or the Medicare Shared Savings Program. Providers that do not participate in these programs will continue to enjoy delayed enforcement pending future rule making. **Comments on the Proposed HHS Disincentives Rule are due no later than January 2, 2024,** and can be submitted electronically [here](#).

This Coppersmith Brief puts the current state of IBR enforcement into context for health care providers, health IT developers and HIN/HIEs and provides practical tips for how to prepare for IBR enforcement through implementation of an IBR compliance program.

TABLE OF CONTENTS

INTRODUCTION	1
IBR BACKGROUND	3
SUMMARY OF THE OIG CMP RULE FOR INFORMATION BLOCKING.....	3
Applicability and Statute of Limitations for CMPs	3
Enforcement Priorities	4
The Investigation Process and Appeals.....	5
What Constitutes a Violation: Single and Multiple Violations.....	6
Determining Penalty Amounts for Violations	7
Individual Liability and Parent Entity Liability	8
Alternatives to CMPs.....	9
SUMMARY OF PROPOSED HHS DISINCENTIVES RULE FOR PROVIDERS	10
Limited Applicability and Request for Information.....	10
CMS Disincentives.....	11
<i>Medicare Promoting Interoperability (PI) Program</i>	<i>11</i>
<i>MIPS: Promoting Interoperability Performance Category (Quality Payment Program)</i>	<i>12</i>
<i>Medicare Shared Savings Program: Accountable Care Organizations (ACOs)</i>	<i>13</i>
Enforcement Priorities	15
The Investigation Process and Appeals.....	16
Multiple Disincentives.....	17
Transparency.....	17
OTHER POTENTIAL CONSEQUENCES FOR VIOLATING THE IBR.....	17
HOW TO GET READY FOR ENFORCEMENT	18
ABOUT THE AUTHORS	20
ENDNOTES.....	21

IBR BACKGROUND

The Information Blocking Rule or IBR (collectively, [42 U.S.C. § 300jj-52](#) and [45 C.F.R. Part 171](#)) prohibits certain actors—that is, health care providers, health IT developers of certified health information technology (including offerors of such health IT), and HIN/HIEs—from engaging in practices that are likely to interfere with the access, exchange or use of electronic health information (EHI) unless the practice is required by law or a regulatory exception applies. The compliance deadline for IBR took effect on April 5, 2021. On October 6, 2022, the option for limiting compliance to EHI identified by the data elements in the USCDI v1 expired. On April 18, 2023, ONC proposed changes to IBR as part of its proposed “Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing” regulation or “HTI-1,” which is pending finalization. You can learn more about HTI-1 in the Coppersmith Brief, [Making Improvements?: ONC’s Proposed Enhancements to the Information Blocking Rule \(HTI-1\)](#). ONC is also planning further substantive changes to IBR with HTI-2, which has not yet been released.

In the meantime, HHS has moved forward with the enforcement structure for IBR. Under the Cures Act, OIG has authority to investigate information blocking claims against all actor types. Following an information blocking investigation, if OIG determines that a health IT developer or HIN/HIE committed information blocking, OIG may impose a civil monetary penalty up to \$1 million per violation; if OIG determines that a health care provider committed information blocking, OIG will refer the provider to the appropriate agency for appropriate disincentives.⁴ A comprehensive summary of the final [OIG CMP Rule](#) and [Proposed HHS Disincentives Rule](#) is set forth below. We also encourage IBR actors to consider OIG’s existing regulatory framework for the imposition and appeal of CMPs (see 42 CFR Parts 1003 and 1005) and the recently updated [OIG General Compliance Program Guidance](#).

SUMMARY OF THE OIG CMP RULE FOR INFORMATION BLOCKING

This section provides a summary of the final OIG CMP Rule and related commentary, including its applicability, OIG enforcement priorities, the investigation process and appeals, analysis of what constitute a violation, how penalty amounts will be determined, individual liability and parent entity liability and alternatives to CMPs.

Applicability and Statute of Limitations for CMPs

The OIG CMP Final Rule sets forth the IBR enforcement structure for health IT developers and HIN/HIEs. Specifically, OIG codified within its existing regulatory framework for CMPs its information blocking authority at [42 CFR 1003.1400](#), [1003.1410](#), and [1003.1420](#). Although OIG may only impose CMPs on health IT developers and HIN/HIEs, OIG investigates claims against, and will make determinations of information blocking by, health care providers as well. Health care providers that meet the regulatory definition of health IT developer or HIN/HIE will also be subject to CMPs with respect to EHI practices done in the capacity of a developer or HIN/HIE. Thus, health care providers should consider the OIG CMP Rule and its interaction with the Proposed HHS Disincentives Rule when preparing for IBR enforcement. Notably, OIG will only impose CMPs for practices that occurred on or after the enforcement start date⁵—September 1, 2023.⁶ For conduct occurring after September 1, OIG has 6 years from the date an actor committed a practice that constitutes information blocking to impose a CMP.⁷

Enforcement Priorities

Only a small portion of the approximately \$87 million dollars OIG was allocated in the 2023 Congressional Budget bill for motor vehicle investigations and child support non-payment cases is allocated for information blocking enforcement,⁸ and OIG is only requesting a modest increase to approximately \$116.8 million for its 2024 budget.⁹ Accordingly, OIG is allocating its resources to certain enforcement priorities. OIG's enforcement priorities include conduct that:

- Resulted in, is causing, or had the potential to cause patient harm (including specific individual harm or harm to a patient population, community or the public);
- Significantly impacted a provider's ability to care for patients;
- Was of long duration;
- Caused financial loss to federal health care programs or other government or private entities; or
- Was performed with actual knowledge, which is of import to health IT developers or HIN/HIEs who may violate the IBR without actual knowledge so long as they should have known they were information blocking. OIG considers conduct with actual knowledge to be more egregious and thus an enforcement priority.¹⁰

OIG further explains that it may evaluate complaints and prioritize investigations that fall within these categories based on the individual allegations or on the sheer volume of claims relating to the same or similar conduct by the same actor. OIG also readily acknowledges that although it has over three decades of experience of CMP enforcement generally, it is new to IBR enforcement. Thus, OIG cautions actors that these priorities may evolve as OIG gains more experience in information blocking. Moreover, they are non-binding and not dispositive to which complaints OIG will pursue.

OIG also provides some insight on how these enforcement priorities may be reflected in the types of complaints it investigates. OIG gives the following example:

[O]ur current anticipated enforcement priorities may lead to investigations of anti-competitive conduct or unreasonable business practices. The ONC Final Rule provides, as examples . . . anti-competitive or unreasonable conduct, such as unconscionable or one-sided business terms for the access, exchange, or use of EHI, or the licensing of an interoperability element. For example, 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. . . . A claim of such conduct would implicate OIG's enforcement priority related to a provider's ability to care for patients. Anti-competitive conduct resulting in information blocking could implicate other enforcement priorities as well, depending on the facts.¹¹

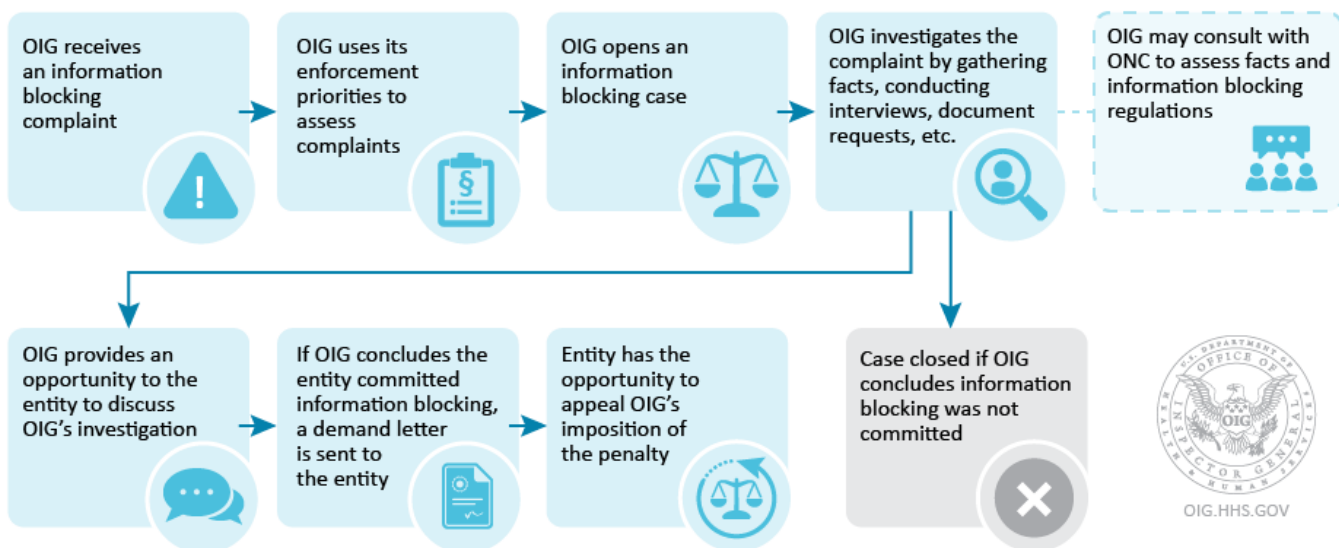
Unfortunately, there is no advisory opinion process that actors may use to seek guidance about IBR application to specific practices. OIG does not currently plan to establish an advisory opinion process regarding the application of the CMP for information blocking, nor does that authority exist under OIG's current advisory opinion powers.¹² However, HHS has included in the Justification of Estimates to the Appropriations Committee for the President's fiscal year (FY) 2024 budget a legislative proposal to grant HHS authority to issue advisory opinions on information blocking practices.¹³

The Investigation Process and Appeals

OIG will work closely with the ONC throughout the complaint and investigative process. Indeed, ONC will continue to operate the [Report Information Blocking Portal](#), and ONC provides a helpful [flow chart](#) on what happens to a complaint after portal submission. OIG may also directly receive complaints from individuals through its [tipline](#) or by individuals calling 1-800-447-8477. OIG has created this diagram on the investigation process.¹⁴

Information Blocking Investigations and Enforcement For Entities Subject to Civil Monetary Penalties

Disclaimer: Non-legal document for educational purposes only.



Throughout the investigative process, OIG may refer the matter to, or consult with, other federal agencies,¹⁵ such as:

- The HHS Office for Civil Rights (OCR), if the information blocking alleged involves the HIPAA privacy, security or breach notification rules.
- The Federal Trade Commission (FTC), if the information blocking is specific to anti-competitive conduct or FTC privacy, breach or security requirements.
- CMS, if the actor is a health care provider that participates in one of the programs for which disincentives may be applied under the Proposed HHS Disincentives Rule (see [below](#)); however, OIG explains in the OIG CMP Rule that it will not use its investigative authority to determine whether the actor is non-compliant with these programs.¹⁶
- Other HHS agencies to avoid duplicate penalties.

OIG does not offer additional guidance regarding how the investigation process may proceed into a complaint of information blocking. However, actors should expect OIG to follow its normal investigative procedures, which may involve requests for information, witness interviews (*e.g.*, patients, employees, vendors, *etc.*), unannounced visits to an actor's place of business, and/or the issuance of subpoenas for records or testimony.

The investigation may conclude with either a dismissal of the information blocking complaint, referral to another

agency, or, if the actor is a health IT developer or HIN/HIE, settlement or the imposition of CMPs. If a CMP is imposed by OIG on a health IT developer or HIN/HIE, that actor may seek an appeal in accordance with existing appeal procedures ([42 CFR Part 1005](#)).

What Constitutes a Violation: Single and Multiple Violations

A significant concern with respect to IBR enforcement is how OIG will determine the number of violations. Health IT developers and HIN/HIEs face up to \$1 million *per violation*.¹⁷ The OIG CMP Rule defines “violation” as “a practice, as defined in [45 CFR 171.102](#), that constitutes information blocking, as set forth in [45 CFR part 171](#).”¹⁸ Thus, a “violation” is:

- An “action or omission” that;
- Except as required by law or covered by an IBR exception, “is likely to interfere with access, exchange, or use of electronic health information;” and
- “If conducted by a health IT developer of certified health IT, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with access, exchange, or use of electronic health information; or
- 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 electronic health information.”¹⁹

Under this definition, OIG will focus on the specific number of actions or omissions taken by an actor. OIG offers the following illustrative examples of how OIG will determine the number of violations:

- A health care provider using technology from a health IT developer (D1) makes a single request to receive EHI for 10 patients through the certified API technology of a health IT developer of health IT (D2). D2 takes a single action to deny the request for all 10 patients. OIG will count this as a single violation subject to the \$1 million cap.²⁰
- A health care provider using health IT supplied by D1 makes multiple, separate requests to receive EHI for several patients via certified API technology supplied by D2. D2 denies each individual request. D2 does not set up the system to deny all requests made by D2. OIG will count each denial as a separate violation. Each separate violation could result in penalties up to the \$1 million cap.²¹
- A health care provider using health IT supplied by D1 makes multiple requests to receive EHI for a single patient via certified API technology supplied by D2. D2 has a technical policy (which OIG refers to as a “system update”) that denies all requests made by anyone using D1’s technology. OIG will consider this to be a single violation (not multiple violations). In this case, OIG explains that the singular action giving rise to the violation is the blanket technical policy that denies all EHI requests made via D1’s health IT. OIG explains that it will not consider each individual denial made pursuant to that system update to be a separate violation.²²

But this example from OIG is contradicted by OIG’s later statements in the commentary to the OIG CMP Rule that while OIG will treat the enactment of a policy as a single violation, “each enforcement of the policy will constitute another, separate violation.”²³ It is unclear whether OIG is drawing a distinction between technical (or systems) policies and administrative policies, or why such a distinction would be material if OIG’s overriding concern is that: “If

the creation or existence of the policy alone is what determined the number of violations, and not the number of times the policy was enforced, large organizations with many customers or significant market share would be able to enact policies—regardless of whether they have been written or formalized—and engage in nationwide conduct constituting information blocking against multiple individuals or entities knowing that the maximum penalty would be the statutory maximum of \$1 million.”²⁴ Thus, notwithstanding OIG’s example in the commentary to the CMP Final Rule, health IT developers and HIN/HIEs should exercise caution before implementing system (technical) policies that deny all types of certain EHI requests, because OIG may conclude that exercising that policy gives rise to multiple violations.

- A health IT developer enters into a software license agreement with a health care provider that requires the provider to pay a fee for exporting patients’ EHI via the capability certified according to 45 CFR 170.315(b)(10) for switching health IT systems. When the provider requests the electronic export, the health IT developer charges the health care provider the fee. OIG would consider this conduct to include two violations: (1) the contract provision for the fee; and (2) charging the fee.²⁵

OIG offers additional examples of how it will determine the number of violations in the OIG Proposed CMP Rule at [85 FR 22979, 22986-87 \(Apr. 24, 2020\)](#).

Importantly, OIG’s determination that conduct constitutes a single violation versus multiple violations does not mean that the CMP imposed on an actor for a single violation will necessarily be less than an CMP imposed on an actor for the multiple violations. OIG will consider the number of individuals affected by a violation—such as an improper system update that results in the denial of all requests made by D1’s technology—as an aggravating circumstance in determining the penalty.

Determining Penalty Amounts for Violations

Aside from the per violation monetary cap, there is no specific mathematical formula that OIG will use to determine CMP amounts. CMP determinations require a facts and circumstances analysis. However, OIG must take into the account the following factors when determining CMPs:

- (a) The nature and extent of the information blocking including where applicable:
 - (1) The number of patients affected;
 - (2) The number of providers affected; and
 - (3) The number of days the information blocking persisted; and
- (b) The harm resulting from such information blocking including where applicable:
 - (1) The number of patients affected;
 - (2) The number of providers affected; and
 - (3) The number of days the information blocking persisted.²⁶

These factors are in addition to, and overlap with, the factors OIG generally considers when determining CMPs under [42 CFR 1003.140](#).²⁷ Accordingly, OIG will also take into account facts and circumstances such as:

- The nature of claims and the circumstances under which they were presented;
- The degree of culpability;
- The history of prior offenses;
- The financial condition of the person presenting the claims;
- The financial condition of the actor and, once OIG proposed a CMP, the individual or entity may request that OIG consider its ability to pay; and
- Such other matters as justice may require.

OIG offers these examples of how it might weight these factors in the context of an IBR penalty calculation:

- With respect to nature of the claims and the circumstances and the nature and extent of the information blocking, OIG may consider: “whether the 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.”²⁸
- With respect to culpability, OIG may consider whether there was actual knowledge or specific intent.²⁹
- With respect to harm, OIG may consider physical or financial harm, as well as the severity and extent.³⁰
- Additionally, OIG will consider whether the information blocking was self-reported, whether the actor took appropriate and timely corrective action, and whether the actor fully cooperated with OIG.³¹

OIG also expressed its intent to reserve the maximum penalty of \$1 million per violation for particularly egregious conduct.³² OIG did not, however, provide examples of what conduct it would consider particularly egregious.

Individual Liability and Parent Entity Liability

Potential IBR liability, and OIG’s enforcement authority, are not limited to entities. The definitions of health IT developer and HIN/HIE include both an “individual or entity,”³³ and OIG is specifically given authority to impose CMPs against “[a]ny individual or entity” that qualifies as such a developer or HIN/HIE.³⁴ However, OIG comments in the OIG CMP Rule suggest that OIG is not focused on pursuing CMPs against individuals.

OIG explains that it will assess individual liability by first determining whether the individual—as opposed to the entity which employs or otherwise engages the individual—meets the actor definition. Using the example of an individual that serves on a HIN/HIE advisory, OIG explains that the “mere act of serving on an advisory board would not mean an individual is a HIN/HIE;”³⁵ rather OIG would consider the following factors:

- The advisory board’s purpose and authority to determine, control, or discretion to administer any requirement, policy, or agreement; and
- The individual’s role, the individual’s authority, and whether the individual determines, controls, or has the discretion to administer any requirement, policy, or agreement as a member of the advisory board.³⁶

If such factors favor a finding that the individual was acting in the capacity of a HIN/HIE, OIG then considers whether **the individual** engaged in the specific practice that constituted information blocking with the requisite level of intent. OIG emphasizes that an individual shall not be determined to have engaged in information blocking with respect to a

practice committed by another individual or entity, suggesting that a HIN/HIE advisory board member shall not be held liable for a practice beyond the authority, determination, control or discretion of the advisory board.³⁷ OIG thus concludes “it is unlikely that an individual serving on a HIN/HIE governance and advisory committee would be subject to information blocking enforcement.”³⁸

OIG does not opine on individual liability for executive leadership or other workforce members of health IT developers or HIN/HIEs in the OIG CMP Rule. However, within this discussion, OIG notes that it is not required to investigate every allegation it receives, and that OIG may decide it is more appropriate to impose CMPs on the entity (as opposed to individuals or both the individual and entity).³⁹ This suggests that at this stage, OIG is more focused on entity-level enforcement.

OIG also offers some commentary on IBR liability for parent entities of subsidiaries that engage in information blocking. OIG explains that if a subsidiary entity acts as the agent of the parent entity, the parent may be subject to CMPs if the subsidiary commits information blocking within the scope of its agency for the parent.⁴⁰ OIG also acknowledges that there may be other instances when information blocking by a subsidiary or affiliate may create CMP liability for the parent, and OIG will consider this on a case-by-case basis.⁴¹ Thus, creating new corporate entities to house developer or HIN/HIE business lines subject to the IBR may not be sufficient to protect a parent entity from IBR liability.

Alternatives to CMPs

OIG does not intend to offer alternatives to CMPs, such as providing technical assistance, additional education or corrective action plans.⁴² Citing its historical position regarding its enforcement of fraud and abuse laws, OIG explains that: “the Federal health care programs are best protected when persons who engage in fraudulent or other improper conduct are assessed a financial sanction. This remedial purpose is at the core of OIG’s administrative enforcement authorities.”⁴³ However, OIG may reconsider this position as they gain more experience. Moreover, OIG anticipates referring matters over to ONC, OCR and other regulatory bodies who may, under their respective authorities, provide individualized education or corrective action plans.

HHS also intends to apply its self-disclosure protocol (SDP) to information blocking, such that health IT developers and HIN/HIEs may self-disclose an IBR violation to resolve CMP liability and allow for lower penalties.⁴⁴ HHS intends to do this by updating its SDP page at <https://oig.hhs.gov/compliance/self-disclosure-info/>. As of the date of this briefing, the webpage has not been updated to reflect IBR self-disclosure. Nor has it been added to OIG’s Information Blocking website at <https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/>. However, OIG explains that when posted, the website will include SDP eligibility criteria, manner and format, submission content requirements and the expected resolution process. Actors interested in self-disclosure prior to this website update may still self-disclose by contacting OIG directly. Self-disclosure is a mitigating factor only. It does not guarantee a lower penalty and would not resolve any liability an actor has under other laws, such as HIPAA or the ONC Certification Program.

SUMMARY OF PROPOSED HHS DISINCENTIVES RULE FOR PROVIDERS

Under the Cures Act, if OIG investigates a health care provider and determines that the provider committed information blocking, OIG is required to refer the provider “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.”⁴⁵ On November 1, 2023, HHS published the [Proposed HHS Disincentives Rule](#) in the Federal Register. The comment period closes on January 2, 2024. This section breaks down the HHS proposal and the potential impact on health care providers, health IT developers and HIN/HIEs.

Limited Applicability and Request for Information

The most striking aspect of the Proposed HHS Disincentive Rule is that it is only a partial enforcement rule for those health care providers who participate in certain CMS programs, namely the Medicare Promoting Interoperability Program (PI) for eligible hospitals and critical access hospitals (CAHs), the Promoting Interoperability performance category of the Merit-based Incentive Payment System (MIPS) (fka EHR Incentive Program) for eligible clinicians, and the Medicare Shared Savings Program for health care providers that are accountable care organizations (ACOs), ACO participants, or ACO providers/suppliers.

Specifically:

- ONC/CMS propose to introduce a new Subpart J (Disincentives for Information Blocking by Health Care Providers) to the IBR, which consists of 3 sections on scope (45 CFR 171.1000), disincentives (45 CFR 171.1001) and notice of disincentives (45 CFR 171.1002). Section 171.1000 provides that this Subpart J “sets forth disincentives that an appropriate agency may impose on a health care provider based on a determination of information blocking referred to that agency by OIG, and certain procedures related to those disincentives.”
- They propose to define “appropriate agency” as “a government agency that has established disincentives for health care providers that [OIG] determines have committed information blocking,” and “disincentive” as “a condition specified in § 171.1001(a) that may be imposed by an appropriate agency on a health care provider that OIG determines has committed information blocking for the purpose of deterring information blocking practices.”⁴⁶
- ONC/CMS further purport to interpret the phrase “authorities under applicable Federal law” from the Cures Act to mean “an appropriate agency may only subject a health care provider to a disincentive established using authorities that could apply to information blocking by a health care provider subject to the authority, such as health care providers participating in a program supported by the authority.”⁴⁷ ONC/CMS have offered this interpretation without regard to the Cures Act’s other requirement that HHS, to the extent possible, ensure that penalties do not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved.⁴⁸

In short, ONC/CMS propose to detail in the IBR—specifically 45 CFR 171.1001—all the specific disincentives health care providers may face under existing federal authorities relating to information sharing if OIG determines they have committed information blocking. Section 171.1001, as proposed, only lists disincentives for health care providers who already participate in the CMS PI Program, the MIPS PI component of the CMS Quality Payment Program, or the Medicare Shared Savings Program.

Health care providers who participate in such CMS programs are only a small proportion of those health care providers who are subject to IBR. IBR broadly defines “health care providers” to include:

[A] hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center (as defined in section 300x–2(b)(1) of this title [42 USC]), renal dialysis facility, blood center, ambulatory surgical center described in section 1395l(i) of this title [42 USC], emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician (as defined in section 1395x(r) of this title [42 USC]), a practitioner (as described in section 1395u(b)(18)(C) of this title [42 USC]), a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe (as defined in the Indian Self-Determination and Education Assistance Act [25 U.S.C. 5301 *et seq.*]), tribal organization, or urban Indian organization (as defined in section 1603 of title 25), a rural health clinic, a covered entity under section 256b of this title, an ambulatory surgical center described in section 1395l(i) of this title [42 USC], a therapist (as defined in section 1395w–4(k)(3)(B)(iii) of this title), and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.⁴⁹

This limited enforcement applicability benefits health care providers who do not participate in such programs by removing the direct regulatory risks of non-compliance and, for those who do participate in these CMS programs, largely limiting the risk of noncompliance to the risks already inherent to their participation in those programs.

However, the limited enforcement structure may undermine HHS’s information sharing goals. For example, many health IT developers and HIN/HIEs are business associates of health care providers who may not participate in these CMS programs, but who control how their EHI is accessed, exchanged and used through the technology platforms and services offered by health IT developers and HIN/HIEs. These business associates cannot use or disclose EHI without permission of their data suppliers, and ONC recognizes that IBR does not require actors to violate their business associate agreements.⁵⁰ Thus, enforcement actions against developers and HIN/HIEs under the OIG CMP Rule may result in little practical change in the industry where the information blocking complained of may originate from data suppliers not subject to enforcement under IBR.

ONC/CMS recognize the importance of establishing disincentives that would apply to all health care providers (as defined by IBR) and seek information from the public to identify specific health care providers and disincentives that may be leveraged under existing federal law.

CMS Disincentives

ONC/CMS propose to add 45 CFR 171.1001 (Disincentives for Information Blocking by Health Care Providers) to the IBR and to update this regulation from time to time to add disincentives. The current proposal for disincentives is as follows:

Medicare Promoting Interoperability (PI) Program

CMS proposes that eligible hospitals and CAHs that participate in the Medicare PI Program would not be a “meaningful

electronic health record (EHR) user” (as defined in 42 CFR 495.4) in an EHR reporting period if OIG refers, during the calendar year of the EHR reporting period, a determination that the eligible hospital or CAH committed information blocking. As a result:

- **Eligible Hospitals.** CMS would reduce the eligible hospital’s payment by three quarters of the applicable percentage increase in the market basket update or rate-of-increase for hospitals. CMS estimates that the median disincentive amount for such eligible hospitals would be \$394,353, and a 95 percent range of \$30,406 to \$2,430,766 across eligible hospitals.⁵¹ CMS further proposes to apply this downward adjustment to the payment adjustment year that occurs 2 years after the calendar year when the OIG referral occurs.⁵²
- **CAHs.** CMS would reduce a CAH’s payment from 101% to 100% of its reasonable costs for the applicable year. CMS proposes to apply this downward adjustment to the payment adjustment year that is the same as the calendar year when the OIG referral occurs.⁵³

In each instance, CMS proposes to tie the disincentive to the date of the OIG referral. CMS considered and rejected using the date of the actual information blocking because the delay between when the information blocking occurred and the date of referral “could complicate the application of the disincentive and would likely necessitate reprocessing of a significant number of claims.”⁵⁴ However, this approach may also have the effect of financially punishing an eligible hospital or CAH for conduct that has long-since been corrected and/or information blocking committed by leadership or personnel no longer with the institution, therefore calling into question its deterrent effect.

Additionally, this approach to disincentives is an “all or nothing approach” that does not consider the severity of the information blocking or aggravating or mitigating factors. For example, an eligible hospital that commits one instance of information blocking would be treated the same as an eligible hospital that commits hundreds of instances of information blocking over a long period of time, unless OIG makes multiple referrals over multiple calendar years/reporting periods. Accordingly, ONC/CMS seek comment on whether there should be multiple disincentives for instances in which OIG determines that information blocking occurred over multiple years.⁵⁵

MIPS: Promoting Interoperability Performance Category (Quality Payment Program)

The Medicare Merit-Based Incentive Payment System (MIPS) is part of the Quality Payment Program authorized by the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA),⁵⁶ which is a payment incentive program for eligible clinicians who provide high-value, high-quality services in a cost-efficient manner. CMS proposes that a health care provider who is a MIPS eligible clinician—as defined in [42 CFR 414.1305](#), *e.g.*, physicians, physician assistants, nurse practitioners, clinical nurse specialists, certified registered nurse anesthetists, certified nurse-midwives, clinical social workers, clinical psychologists, registered dietitians or nutrition professionals, physical/occupational therapists or qualified speech-language pathologist⁵⁷ and including groups—would not be a “meaningful EHR user” (as defined at [42 CFR 414.1305](#)) in a performance period if OIG refers, during the calendar year of the reporting period, a determination that the MIPS eligible clinician committed information blocking. CMS further proposes that such a clinician would be given a zero score on the Promoting Interoperability performance category of MIPS, which is typically one quarter of the total final composite performance score.⁵⁸ Because the applicable MIPS payment year is 2 calendar years after the

performance period, CMS will apply the disincentive two years after the OIG referral. CMS estimates the median individual disincentive amount of \$686 per eligible clinician and a 95 percent range (the 2.5th to 97.5th percentile of estimated disincentive amounts) of \$38 to \$7,184 across all eligible clinicians (including those who may have been in a group).⁵⁹

With respect to groups (including virtual groups), CMS notes that “MIPS eligible clinicians who submit data as a part of a group or virtual group and individually will be evaluated as an individual and as a group for all performance categories.”⁶⁰ CMS further explained during its November 15, 2023, public webinar that for sites who do group reporting under MIPS, if one eligible clinician is found to have engaged in information blocking, this will affect the entire group if they choose to do group reporting.⁶¹ Using an estimated median group size of six clinicians, CMS estimates a group disincentive of \$4,116 and a range of \$1,372 to \$165,326 for group sizes ranging from two to 241 clinicians (the estimated 2.5th to 97.5th percentile of group sizes). With respect to eligible clinicians that may be subject to higher-than-median disincentives, CMS also simulated estimates for a median-sized group of six clinicians and an estimated 75th percentile per-clinician disincentive amount of \$1,798, with an estimated group disincentive of \$10,788.⁶² Of course, the actual amount will vary based on individual clinician payments and group sizes.

Similar to the disincentives for eligible hospitals and CAHs that participate in the PI Program, CMS proposes to apply the disincentive based on the date of the OIG referral (as opposed to the date of the information blocking) to avoid payment complications and the reprocessing of claims.⁶³ However, it is unclear how OIG or CMS will properly attribute eligible clinicians who are found to have engaged in information blocking and either (1) participate in multiple different groups at the time of the OIG referral, or (2) change or leave groups after engaging in the information blocking that serves as the basis for the later OIG referral. This disincentive system also cannot be adjusted to reflect the severity of the information blocking or to account for aggravating or mitigating circumstances. Accordingly, ONC/CMS also seek comment on whether there should be multiple disincentives for instances in which OIG determines that information blocking occurred over multiple years.⁶⁴

Medicare Shared Savings Program: Accountable Care Organizations (ACOs)

The Medicare Shared Savings Program is a voluntary program that encourages groups of doctors, hospitals, and other health care providers to come together as an ACO to give coordinated, high-quality care to their Medicare beneficiaries. CMS proposes to revise the Medicare Shared Savings Program such that a health care provider who is an ACO, ACO participant, or ACO provider/supplier, who is determined by OIG to have committed information blocking, would be barred from participating in the Medicare Shared Savings Program for at least 1 year.⁶⁵ CMS expects such a result may cause a provider to be removed from an ACO or prevented from joining an ACO; and in the instance where a provider is an ACO, this would prevent the ACO’s participation in the Medicare Shared Savings Program during the duration of the disincentive. This disincentive would, in turn, deprive these health care providers from receiving revenue that they might have otherwise earned had they been able to participate.

Specifically, CMS proposes to amend 42 CFR 425.208(b) to require an ACO—as well as ACO participants, ACO providers/suppliers, and other individuals or entities performing functions or services related to ACO activities—to agree to comply with “[t]he information blocking provision of the 21st Century Cures Act (42 U.S.C. 300jj–52).”⁶⁶ This is notable (and arguably beyond the intended scope of this enforcement rule) because it expands the requirement to

comply with IBR beyond IBR actors to include ACOs (that might otherwise not qualify as an IBR actor) and other types of individuals or entities involved with ACOs, at least under CMS's programmatic authority. CMS further proposes to amend 42 CFR 425.305 and 42 CFR 425.218, respectively, to give CMS express authority to consider as part of the program integrity history screening, and as grounds for termination of program participation, any violation of applicable law relevant to ACO operations, including those specified in the amended 42 CFR 425.208(b).⁶⁷

CMS proposes to apply this disincentive to the first performance year after CMS receives a referral of an information blocking determination from OIG.⁶⁸ CMS further proposes to allow CMS to apply the disincentive for additional performance years if, for example, OIG makes subsequent determinations of information blocking.⁶⁹ CMS offers this example of how it would apply this disincentive as part of its ordinary program integrity screenings of ACOs:

CMS performs a program integrity screening of ACOs, ACO participants, and ACO providers/suppliers as part of the annual application/change request process for new and existing ACOs, which typically occurs between May and October during the performance year. In the case of the new addition of an ACO participant (TIN) to an ACO's participant list, CMS would prevent the TIN from joining the ACO as an ACO participant if the program integrity screening reveals that the TIN has engaged in information blocking, as determined by OIG. In the case of an existing ACO participant, CMS would notify the ACO that an ACO participant or an ACO provider/supplier had committed information blocking, as determined by OIG, so the ACO can remove the ACO participant or ACO provider/supplier from its ACO participant list or ACO provider/supplier list, as applicable. If the TIN were to remain on the ACO participant list or ACO provider/supplier list when the ACO certifies its ACO participant list for the next performance year, then CMS would issue a compliance action to the ACO. Continued noncompliance (for example, failure to remove the TIN) would result in termination of the ACO's participant agreement with CMS, as the ACO would have failed to enforce the terms of its ACO participant agreement.⁷⁰

....

After the completion of the last performance year in which the disincentive was applied, an ACO may submit a change request to add the TIN or include the NPI on its ACO participant list or ACO provider/supplier list, as applicable, for a subsequent performance year, and CMS would approve the addition, assuming that all other Shared Savings Program requirements for adding a TIN or NPI are met, so long as (1) OIG has not made any additional determinations of information blocking, and (2) the ACO provides assurances (in the form and manner required by CMS) that the information blocking is no longer ongoing and that the ACO has put safeguards in place to prevent the information blocking that was the subject of the referral. If, however, OIG made and referred an additional information blocking determination (that is either related or unrelated to the previous OIG referral) in a subsequent year or the ACO cannot provide assurance that the information blocking has ceased, then CMS would continue to deny participation.⁷¹

CMS has considered and rejected applying the disincentive retroactively on the ground that it would be "impractical and inequitable for CMS to apply the disincentive retrospectively or in the same year in which CMS received a referral from

OIG” because it “would unfairly affect other ACO participants that did not commit the information blocking and likely were not aware of the information blocking.”⁷² However, CMS also recognizes that its proposed approach may mean that a disincentive is applied substantially after the information blocking occurred and after a provider may have otherwise been subject to a disincentive under MIPS (or other appropriate agency). Accordingly, CMS is seeking comment on whether it should apply an alternative policy whereby CMS would not apply a disincentive in certain circumstances despite an OIG information blocking determination, such as if a significant amount of time has passed (such as 5 years) and the provider has given assurances that appropriate safeguards are in place to prevent a reoccurrence of information blocking.⁷³

More specifically, CMS seeks comment on an alternative policy in which CMS—before applying a disincentive—would consider the OIG determination of information blocking as well as the following factors:

- The nature of the health care provider’s information blocking;
- The health care provider’s diligence in identifying and correcting the problem;
- The time since the information blocking occurred;
- The time since OIG’s determination of information blocking; and
- Other factors.⁷⁴

Individuals and entities subject to a disincentive under this proposed provision may be able to appeal application of the disincentive through CMS’s review process (42 CFR 425.800); however, OIG’s underlying information blocking determination would not be eligible for review.⁷⁵

Enforcement Priorities

As noted above, OIG has authority to investigate IBR complaints against all actor types, including health care providers. ONC/CMS note in the commentary to the Proposed HHS Disincentive rule that the OIG’s enforcement priorities for providers will be the same as for health IT developers and HIN/HIEs. Specifically, OIG will prioritize information blocking conduct that:

- Resulted in, is causing, or had the potential to cause patient harm (including specific individual harm or harm to a patient population, community or the public);
- Significantly impacted a provider’s ability to care for patients;
- Was of long duration; or
- Caused financial loss to federal health care programs, or other government or private entities.⁷⁶

OIG does not intend to use the fifth priority listed for enforcement against health IT developers and HIN/HIEs—that is, conduct performed with actual knowledge—because actual knowledge is a required intent element for OIG to find that a provider has committed information blocking in the first instance. OIG will use its significant experience and expertise in enforcing fraud and abuse laws to determine whether this element of an IBR claim is met.⁷⁷

Please see the section on [Enforcement Priorities](#) in the [Summary of the OIG CMP Rule for Information Blocking](#) for more information on how OIG may evaluate and prioritize information blocking claims.

The Investigation Process and Appeals

The OIG investigation process from complaint up to OIG's determination will be the same for health care providers as for the other actors. Please see the section on the [Investigation Process and Appeals](#) in the [Summary of the OIG CMP Rule for Information Blocking](#) for more information on this process. The only differences for providers are that if OIG determines the provider has committed information blocking, OIG will refer that provider to the appropriate agency for disincentives and the provider's appeal rights (if any) must be exercised through that agency's appeal process. Notably, the appeals process applicable to the imposition of CMPs against health IT developers and HIN/HIEs does not apply to an OIG determination that a provider has committed information blocking.⁷⁸ It is thus unclear whether there is any actual administrative appeal process to challenge an OIG determination of information blocking. It is also unclear whether OIG will even investigate providers who are not subject to the proposed disincentives.

In making a referral to an appropriate agency for disincentive, OIG will provide the following information to the agency:

- The dates when OIG has determined the information blocking violation(s) occurred;
- OIG's analysis to explain how the evidence demonstrates the health care provider committed information blocking (that is, that the elements of an IBR claim are established);
- Copies of evidence collected during the investigation;
- Copies of transcripts and video recordings (if applicable) of any witness and affected party testimony;
- Copies of documents OIG relied upon to make its determination that information blocking occurred; and
- Any additional information OIG desires to provide, to the extent permitted by applicable law.⁷⁹

Following such a referral, ONC/CMS propose that the agency will be required to give the provider the following notice (using usual methods of communications) that includes all of the following information:

- A description of the practice or practices that formed the basis for the determination of information blocking referred by OIG;
- The basis for the application of the disincentive or disincentives being imposed;
- The effect of each disincentive; and
- Any other information necessary for a health care provider to understand how each disincentive will be implemented.⁸⁰

With respect to ACOs who are not engaged in information blocking, but which may have an ACO participant or ACO provider/supplier who has committed information blocking, CMS explains in commentary to the Proposed HHS Disincentives Rule that it will also notify the ACO so that the ACO may take remedial action, such as removing the ACO participant from the ACO participant list or the ACO provider/supplier from the ACO provider/supplier list as required by the ACO participant agreement.⁸¹

A provider subject to an agency disincentive may have the right to appeal the disincentive if the agency that applies the disincentive provides for such an appeal.⁸² However, this appeal right presumably would not extend to the underlying OIG determination of information blocking.⁸³

Multiple Disincentives

An entity or individual found by OIG to have committed information blocking may find themselves subject to multiple disincentives. Notwithstanding the Cures Act's general requirement that HHS (to the extent possible) ensure that penalties (with respect to all actor types) do not duplicate penalty structures that would otherwise apply to information blocking, ONC/CMS notes that the specific statutory provision on provider disincentives does not expressly limit the number of disincentives that an appropriate agency can impose on a health care provider. As such, ONC/CMS proposes to allow providers who commit information blocking to be subject to multiple disincentives as set forth in a single notice or multiple notices,⁸⁴ provided that the appropriate agency has jurisdiction over the provider and has established a penalty structure through a notice and comment period.⁸⁵ ONC/CMS specifically seek comment on whether cumulative penalties are an appropriate and necessary deterrent for information blocking by providers.

Transparency

ONC/CMS also propose a new Subpart K (Transparency for Information Blocking Determinations, Disincentives, and Penalties) that would create a "wall of shame" for all actor types that OIG finds have committed information blocking.⁸⁶ Specifically, ONC proposes to post on its public website the following information about information blocking actors in order to provide transparency into how and where information blocking is occurring within the health care industry:

- **Health Care Providers Subject to Disincentives.** ONC proposes to post on its public website the following information about a health care provider that has been subject to a disincentive: name; business address; the practice found to be information blocking; the disincentive(s) applied; and where to find any additional information about the determination that is publicly available via the U.S. government. Such information would not be posted prior to imposition of the disincentive. Notably, health care providers who commit information blocking, but who are not subject to a disincentive under this partial enforcement rule, would not have their information posted on the ONC website. Additionally, health care providers who have a statutory right to review public information about themselves—such as MIPS eligible clinicians who have the right to review information about their MIPS performance prior to it being published in the CMS Compare Tool—would have a right to review their information prior to its posting on the ONC website.⁸⁷
- **Health IT Developers and HIN/HIEs.** ONC also proposes to post on its public website the following information about a health IT developer or HIN/HIE that has been determined by OIG to have committed information blocking: the type of actor; actor's legal name and any alternative or tradenames (like dbas); a description of the practice; and where to find any additional information about the determination that is publicly available via the U.S. government, such as information about any court actions.⁸⁸ Such information would not be posted prior to OIG entering into a resolution agreement for the CMP liability or imposition of a CMP that has become final under [42 CFR Part 1003](#).

OTHER POTENTIAL CONSEQUENCES FOR VIOLATING THE IBR

CMPs for health IT developers and HIN/HIEs, and HHS disincentives for health care providers, are only one source of potential federal regulatory liability for actors subject to the IBR. IBR violations may give rise to other forms of liability, which should be considered by actors when assessing IBR enforcement and the risks of noncompliance.

For example, depending on the actor and facts and circumstances giving rise to the IBR violation, other potential consequences may include:

- ONC acting against an individual or entity that is a health IT developer participating in the ONC Certification Program, including up to termination of the developer's certificate.
- OCR imposing penalties under HIPAA's enforcement structure for violations of an individual's HIPAA right of access or a business associate's obligation to safeguard the accessibility of protected health information.
- FTC imposing penalties under its authorities specific to anti-competitive conduct.
- The Department of Justice (DOJ) taking action under the False Claims Act if there are materially false attestations or antitrust violations.
- State regulatory liability or civil litigation under state laws that similarly prohibit or protect against information blocking.

HHS is required, to the extent possible, to ensure that the penalties imposed under either the OIG CMP Rule or the future finalized HHS Disincentives Rule do not duplicate the penalty structures that would otherwise apply to information blocking and the type of individual or entity involved.⁸⁹ But this statutory restraint is not absolute, and it does not preclude another federal agency (or other enforcement authority) from imposing other requirements on an actor, such as a corrective action plan, in lieu of a penalty. OIG explains in the commentary to the OIG CMP Rule that:

For example, OIG may refer an allegation to OCR for consultation regarding the health privacy and security rules or for OCR to address under its HIPAA authorities. Similarly, OIG may refer an allegation to ONC to address under its direct review authority, under which ONC could impose a corrective action plan. ONC also stated in the ONC Final Rule that ONC's and OIG's respective authorities are independent and that either office may exercise its authority at any time. . . . Thus, OIG's enforcement action will only include a CMP, while ONC could pursue a separate enforcement action within its authority, which could include a corrective action plan.⁹⁰

Thus, in considering IBR enforcement, actors should also consider whether they are subject to other federal authorities or state jurisdictions in which a determination of information blocking by OIG may give rise to other sources of liability.

HOW TO GET READY FOR ENFORCEMENT

Actors of all types and sizes can get ready for IBR enforcement by implementing and monitoring an IBR compliance program as part of its larger health care compliance program by:

- Establishing an interdisciplinary information blocking workgroup (including clinical, compliance, legal, security and IT) that is responsible for implementing and monitoring IBR compliance through the organization;
- Educating and training individuals at all levels, including Board members, on IBR compliance and what to do in the event of an OIG request for information or other investigative action (such as an unannounced site visit or subpoena);


The logo for Coppersmith Brockelman Lawyers is centered at the top of the page. It features the name 'COPPERSMITH' above 'BROCKELMAN' in a large, white, sans-serif font. A thin white horizontal line separates the two names. Below 'BROCKELMAN', the word 'LAWYERS' is written in a smaller, white, sans-serif font. The background of the logo is a dark blue image of a city skyline.

COPPERSMITH BROCKELMAN

LAWYERS

- Identifying your organization’s actor type (or types) and whether your organization participates in CMS programs subject to IBR disincentives such as the Medicare PI Program, MIPS, or the Medicare Shared Saving Programs. For larger organizations with parent/affiliate relationships, you’ll also want to assess whether affiliates are subject to the IBR and whether their conduct may be imputed to the parent organization;
- Routinely identifying and assessing the organization’s EHI sources, technology stack, and EHI practices for IBR compliance gaps and addressing those gaps, including updating health information policies and procedures as well as contracts involving the access, exchange or use of EHI or licensing of interoperability elements;
- Routinely evaluating and updating external-facing communications and messaging to reflect how your organization manages EHI access, exchange and use under the laws that apply to your organization and the technology stack currently available to you; and
- Keeping key records regarding EHI practices, such as policies, contracts, infeasibility determinations, and important email communications, for at least six years. OIG may seek CMPs for up to 6 years from the date an actor committed the practice constituting information blocking, and actors bear the burden of proof for affirmative defenses (*e.g.*, safe harbor protection under an IBR exception) and mitigating circumstances by a preponderance of the evidence. Health IT developers that participate in the ONC Certification Program must also retain all records and information necessary to demonstrate compliance for 10 years from the date of certification.

If you have questions or concerns about your organization’s readiness for IBR enforcement, please contact us at msoliz@cblawyers.com.

The logo for Coppersmith Brockelman Lawyers is centered at the top of the page. It features the name 'COPPERSMITH BROCKELMAN' in a large, white, sans-serif font, with a thin white horizontal line separating the two words. Below this, the word 'LAWYERS' is written in a smaller, white, sans-serif font. The background of the logo is a dark blue, semi-transparent image of a city skyline with various buildings and trees.

COPPERSMITH BROCKELMAN

LAWYERS

ABOUT THE AUTHORS

[Melissa \(Mel\) A. Soliz](#), a partner with Coppersmith Brockelman, is highly sought out for her deep expertise on data privacy and interoperability issues ranging from HIPAA and 42 CFR Part 2 compliance to the ONC Information Blocking Rule, TEFCA (the Trusted Exchange Framework and Common Agreement) and CMS interoperability mandates. Her practice also focuses on health information exchange and networks, health IT contracting, data breaches and OCR investigations, as well as clinical research compliance and contracting. Mel is President of the Arizona Society of Healthcare Attorneys (AzSHA) and is recognized by Chambers USA, Best Lawyers®, Southwest Super Lawyers: Rising Stars®, and Phoenix Magazine Top Lawyer for her work in health law.

[Benjamin \(Ben\) Yeager](#) is an associate attorney with Coppersmith Brockelman focused on health care and data privacy law. Ben helps clients navigate the intricate landscape of health data privacy, security, breach reporting, and interoperability laws, including HIPAA, the ONC Information Blocking Rule, state health information confidentiality, and new consumer data privacy laws. Ben advises clients on matters such as HIPAA Business Associate Agreements and website privacy policies and assists clients with federal and state government investigations related to data breaches.

*By the way, you know the Coppersmith Briefs are not legal advice, right? Right!
Check with your attorney for legal advice applicable to your situation.*

ENDNOTES

¹ See [ONC, Information Blocking Claims: By the Numbers \(last visited Dec. 1, 2023\)](#).

² [88 FR at 42827](#).

³ 21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking, [88 FR 74947](#) (Proposed Nov. 1, 2023).

⁴ [42 USC 300jj-52\(b\)\(2\)](#).

⁵ [88 FR at 42827](#).

⁶ [Id.](#)

⁷ Section 3022(b)(2)(C) of the Public Health Service Act (PHSA), 42 USC 300jj-52, requires that the CMP for information blocking follow the procedures under section 1128A of the SSA, [88 FR at 42820](#), and section 1128A(c)(1) requires that an action for CMPs be initiated within 6 years from the date the violation occurred, [88 FR at 42826](#).

⁸ In 2023, only approximately 5% of the budget allocated to OIG was dedicated to information blocking activities. Compare [Consolidated Appropriations Act, 2023, HR 2617 \(117th Congress, 2d Sess.\)](#) at 1044, with [HHS OIG Fiscal Year 2023 Justification of Estimates for Congress](#) at 21.

⁹ [HHS OIG Fiscal Year 2024 Justification of Estimates for Congress](#) at 18.

¹⁰ See [88 FR at 42822–23](#).

¹¹ [Id. at 42823](#).

¹² [Id. at 42825](#).

¹³ [Id.](#)

¹⁴ [OIG, Information Blocking \(last visited Dec. 3, 2023\)](#).

¹⁵ [88 FR at 42823–24](#).

¹⁶ [Id. at 42824](#).

¹⁷ [42 CFR 1003.1410](#).

¹⁸ [42 CFR 1410\(a\)](#).

¹⁹ [45 CFR 171.102 “Practice”](#); [42 CFR 171.103](#) (defining Information Blocking).

²⁰ [88 FR at 42831](#).

²¹ [Id.](#)

²² [Id.](#)

²³ [Id. at 42832](#).

²⁴ [Id.](#)

²⁵ [Id. at 42831](#).

²⁶ [42 CFR 1003.1420](#).

²⁷ [88 FR at 42833](#).

²⁸ [Id.](#)

²⁹ [Id.](#)

³⁰ [Id.](#)

³¹ [Id.](#)

³² [Id. at 42834](#).

³³ See [45 CFR 171.102 “Health IT developer of certified health IT”, “Health information network or health information exchange”](#).

³⁴ [42 USC 300jj-52\(b\)\(2\)\(A\)](#).

³⁵ [88 FR at 42828](#).

³⁶ [Id.](#)

³⁷ [Id. at 42828–29.](#)

³⁸ [Id. at 42828.](#)

³⁹ [Id. at 42829.](#)

⁴⁰ [Id.](#)

⁴¹ [Id.](#)

⁴² [Id. at 42824.](#)

⁴³ [Id.](#)

⁴⁴ [Id.](#)

⁴⁵ [42 USC 300jj-52\(b\)\(2\)\(B\).](#)

⁴⁶ Proposed HHS Disincentives Rule, 88 FR at 74969 “[Appropriate agency](#),” “[Disincentive](#)”.

⁴⁷ [Id. at 74951.](#)

⁴⁸ [42 USC 300jj-52\(D\)\(4\).](#)

⁴⁹ [45 CFR 171.102 “Health care provider”](#) (“Health care provider has the same meaning as ‘health care provider’ in [42 USC 300jj.](#)”); see also [ONC Information Blocking: Health Care Provider Definition and Cross-Reference Table.](#)

⁵⁰ HealthIT.gov Frequently Asked Questions, [Do the information blocking regulations require actors to violate existing business associate agreements in order to not be considered information blockers?](#) (Updated Apr. 9, 2021).

⁵¹ Proposed HHS Disincentives Rule, [88 FR at 74957.](#)

⁵² [Id.](#)

⁵³ [Id.](#)

⁵⁴ [Id.](#)

⁵⁵ [Id.](#)

⁵⁶ [Pub. L. 114–10](#) (April 16, 2015).

⁵⁷ Although eligible clinicians include “qualified audiologists,” these clinicians are not “health care providers” within the meaning of IBR and thus are not subject to disincentives. Proposed HHS Disincentives Rule, [88 FR at 74959.](#)

⁵⁸ [Id. at 74961.](#)

⁵⁹ [Id. at 74960.](#)

⁶⁰ [Id. at 74962.](#)

⁶¹ [ONC Webinar, Information Blocking Disincentives Proposed Rule Information Session](#) (Nov. 15, 2023, 1:30 p.m.).

⁶² Proposed HHS Disincentives Rule, [88 FR at 74960.](#)

⁶³ [Id. at 74961.](#)

⁶⁴ [Id. at 74962.](#)

⁶⁵ [Id. at 74964.](#)

⁶⁶ [Id. at 74968.](#)

⁶⁷ [Id.](#)

⁶⁸ [Id. at 74965.](#)

⁶⁹ [Id.](#)

⁷⁰ [Id.](#)

⁷¹ [Id.](#)

⁷² [Id.](#)

⁷³ [Id.](#)

⁷⁴ [Id. at 74966.](#)

⁷⁵ [Id.](#)

⁷⁶ [Id. at 74951.](#)

⁷⁷ [Id. at 74951–52.](#)

COPPERSMITH BROCKELMAN

LAWYERS

⁷⁸ [42 USC 300jj-52\(b\)\(2\)\(C\)](#).

⁷⁹ [88 FR at 74952](#).

⁸⁰ [Id. at 74969](#).

⁸¹ [Id. at 74965](#).

⁸² [Id. at 74953](#).

⁸³ [See, e.g., id. at 74966](#).

⁸⁴ [Id.](#)

⁸⁵ [Id. at 74951](#).

⁸⁶ [Id. at 74969](#).

⁸⁷ [Id. at 74953–54](#).

⁸⁸ [Id. at 74954](#).

⁸⁹ [42 USC 300jj-52\(d\)\(4\)](#).

⁹⁰ [88 FR at 42824](#).