LEAVITT PARTNERS
An HMA Company

AVIA

The Block Stops Here!

Policy Proposals for Cracking Down on Information Blocking

EXECUTIVE SUMMARY

Information blocking continues to hinder timely access to electronic health data for patients, providers, payers, and the federal government. While regulations required by the 21st Century Cures Act and promulgated by the US Department of Health and Human Services (HHS) prohibit interference with data exchange, in practice information blocking remains largely unchecked. Inadequate enforcement resources have delayed investigations and ambiguous statutory provisions have made it difficult for HHS to establish specific information blocking disincentives for all healthcare providers.[1] To address these issues, sector-specific reforms are necessary, including:

- Congressional action to create a unified and simpler penalty structure and fund enforcement
- Assistant Secretary for Technology and Policy/Office of the National Coordinator (ASTP/ONC) authority to issue binding guidance (e.g., advisory opinion authority) and strengthen certification requirements
- Office of Inspector General (OIG) resourcing to investigate and act

[1] In addition to issuing the following recommendations, we acknowledge and applaud HHS and its subagencies for its recent information blocking enforcement alert, which signaled to the industry that this administration is taking enforcement of information blocking rules seriously. In tandem with this enforcement alert, we urge the administration to enact the policy recommendations we provide in this paper. We believe that these policy changes—in tandem with the administration's prioritization of this issue—will result in a systemic reduction in the practice of information blocking.

- Until Congress acts, the Centers for Medicare & Medicaid Services (CMS) must continue rulemaking to establish all disincentives for regulated providers
- Industry compliance through default data sharing

Implementing the above reforms will improve incentives, accountability, and progress toward a unified health data system. This paper summarizes legal definitions of information blocking by Congress and HHS, outlines current enforcement challenges, and presents recommendations for improving federal enforcement based on industry discussions.

Information blocking is not just a compliance challenge. It strikes at the core of patient safety, trust, and operational performance. When data are delayed or withheld, the consequences include medical errors, redundant tests, higher costs, and care fragmentation. Patients experience frustration and compromised outcomes when they cannot access their records. Clinicians face barriers to delivering timely, coordinated care. Payers struggle to manage population health. Information technology (IT) vendors struggle to serve their clients. Networks are left without critical data needed for systemwide functions.

WHAT IS INFORMATION BLOCKING?

Over the last 20 years, the healthcare industry, specifically providers, payers, and the IT systems that serve them, have sought to modernize how clinical and claims data are captured and exchanged. While the industry has made great strides in getting the right information to the right stakeholder at the right time, there are still too many examples of stakeholders being unable or unwilling to share data, which slows or stymies the use of health data in critical scenarios.

Consider the following real-life examples:

- A patient requests access to personal health information but encounters delays or denials of access from the primary care provider, compromising their ability to seek a second opinion from another doctor
- A specialist receives a patient referral and requests the patient's medical records from the primary care provider, but encounters delays or denials in accessing those records—compromising the ability of the specialist to properly care for the patient
- A stage 4 colon cancer patient who wants to share personal health data with an organization that is starting a new clinical trial that could save the patient's life but finds that the hospital's internal data-sharing policies or electronic health record (EHR) technology makes it difficult or impossible to share that data

These are all examples of information blocking, which prevents information from flowing to the right place at the right time. Although the federal government has taken some steps to address information blocking, rules curtailing the practice are largely left unenforced.

The healthcare ecosystem is rapidly advancing toward a modern data infrastructure where the data and information access issues outlined above can be solved; however, they will only be fully addressed when we eliminate the incentives for entities to information block consumers, patients, caregivers, providers (even providers that compete in the same market), technology vendors (even those that have similar products), health insurers, pharmacies, and health information networks and exchanges.

This white paper provides recommendations that, if implemented, will help to curtail information blocking. Some of these recommendations involve more robust enforcement of current rules, while others entail additional modifications and updates to rules already enacted. We strongly encourage Congress and HHS to prioritize these activities. Technology is on the way to doing its part. It's now time for industry and government to do theirs.

WHAT HAS BEEN DONE TO TRY AND PREVENT INFORMATION BLOCKING VIA FEDERAL POLICY?

In 2004, President George W. Bush issued an executive order that called for the transition to EHRs and established the Office of the National Coordinator.[2] The Office was statutorily codified in the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).[3] Congress granted ONC additional authorities in the 21st Century Cures Act, including various requirements to establish regulations related to information blocking, create the Trusted Exchange Framework and Common Agreement (TEFCA), and facilitate consumer access to a longitudinal health record.[4] The Biden Administration expanded the scope and mandate for ONC while elevating the National Coordinator position to the Assistant Secretary for Technology Policy and expanding the functions of that position.[5]

One of the first instances of federal interest in prohibiting information blocking was the portion of the 21st Century Cures Act, passed by Congress in 2016, which gave additional responsibilities to ONC (now ASTP/ONC). As part of these actions, Congress mandated that certain "actors," including providers, health IT developers, exchanges, and networks, avoid practices that would be "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information."[6]

This prohibition on information blocking changed the expectation for these regulated entities by moving away from a "may share" data exchange paradigm to a "must share" paradigm (subject to limited exceptions). With these requirements, Congress hoped to advance the ability of consumers, patients, caregivers, providers, payers, networks, and others to access critical information needed for care delivery, care management, payment, consumer use, and myriad other purposes.

---

[2] Executive Order 13335

[3] Public Law No: 111-5

[4] Public Law No: 114-255

[5] See: Statement of Organization, Functions, and Delegations of Authority; Office of The National Coordinator for Health Information Technology; A Notice by the Health and Human Services Department on 07/29/2024

[6] See U.S.C. 42 § 300jj–52.

The subsequent Cures Act Final Rule issued by ASTP/ONC to effectuate limitations on information blocking further defined such activities as information blocking for a health IT developer or health information exchange if the entity knows, *or should know,* that the activity is likely to interfere with the access, use, or exchange of electronic health information (EHI). The rule additionally defined information blocking for providers only if the provider has *actual* knowledge that the practice is unreasonable and likely to interfere with the access, use, or exchange of EHI.

HOW IS THE CURRENT STATE WORKING?

Current Successes and Challenges with Information Blocking Enforcement

Since the passage of the Cures Act and the promulgation of various information blocking rules and amendments from HTI-1, the industry has seen some success but many challenges as the federal government seeks to curtail information blocking practices.

Some aspects of the current state are working well. ASTP/ONC has a clear complaint acceptance process and a robust data feed where individuals can see the number and type of complaint submitted.[7] Additionally, ASTP/ONC has produced FAQs, fact sheets, and educational documents that support entities subject to information blocking enforcement.

Info Blocking: Current Process

	**Has information blocking occurred?**
	ASTP receives an information blocking complaint.
	ONC refers the complaint to OIG.
	OIG determines if the complaint concerns an "Actor" as defined by the 21st Century Cures Act.
	If the "Actor" is a health provider, for which disincentives have been created, OIG must determine if the provider had actual knowledge that their behavior blocked the flow of information.
	If the "Actor" is a health IT developer or HIE/HIN, OIG must determine if they knew, or should have known that their behavior was likely to interfere with the flow of information.

[7] See: https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers

	What penalty could apply?
	If OIG determines that a regulated health provider has engaged in information blocking, HHS may be subject to "appropriate disincentives." ***Note:*** *Only a subset of providers have identified disincentives.* ***Note:*** *All penalties are retained by CMS or HHS.*
	If OIG determines that a Network, Exchange, or other Certified Health IT has engaged in information blocking, it may impose civil monetary penalties. ***Note:*** *All CMP's are returned to the Treasury.*
	For Certified Health IT, ONC may also take action under the CEHRT program.
	Note: *HHS has not yet identified "appropriate disincentives" for many provider "actors" such as labs, pharmacies, ambulance providers, and others.*

Nonetheless, enforcing information blocking has been almost nonexistent. There has been limited reporting of information blocking complaints compared to the scale of the problem, confusing expectations for regulated entities, and insufficient resources for federal regulators to conduct investigations of information blocking complaints—resulting in almost no enforcement.[8]

This situation has led to an uncomfortable reality for both federal regulators and regulated entities. Federal regulators are unable to fully enforce the law due to few submissions of information blocking complaints and limited resources to investigate the complaints that are submitted. Regulated entities are unsure of their regulatory requirements to facilitate information sharing, and commit information blocking without realizing it. All of this results in consistent barriers in accessing, using, and exchanging EHI. This situation also has led to ongoing frustration for providers that still cannot access critical, time-sensitive information about a patient sitting in their exam room, as well as for patients and consumers. It is also a challenge for the technology vendors that serve patients and consumers when they cannot connect to a data source with critical lab or pharmacy information.

An additional challenge to information blocking enforcement, unusual for federal regulations, is the number of agencies that participate in this work.

[8] 45 CFR Parts 170 and 171 — Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule, published in the Federal Register on January 9, 2024 (89 FR 1076), effective March 11, 2024.

- **ASTP/ONC** is responsible for promulgating regulations on what constitutes information blocking. They also support providers, networks, and developers through the release of FAQs about what constitutes information blocking in real-world scenarios. Finally, they support the reporting mechanism through which individuals or entities may report information blocking and escalate credible complaints to OIG.
- **OIG** promulgated the rule for health IT developers and networks establishing civil monetary penalties (CMPs).[9] It is also tasked with investigating the complaints passed to it by ASTP/ONC or reported to the OIG hotline for developers, networks, and providers. Through their investigation process they may impose CMPs on networks or developers and may refer providers found in violation to the Centers for Medicare & Medicaid Services (CMS).
- **CMS** (among other HHS agencies) is responsible for coordinating with ASTP/ONC on various information blocking rules as well as identifying, through rulemaking, what appropriate disincentives may be established for providers participating in CMS programs.[10] If OIG makes an information blocking finding against a specific provider, CMS is responsible for imposing the penalty on the provider, consistent with the disincentive regulations.
- The HHS Office for Civil Rights (**OCR**) is also involved, from a technical assistance perspective, in information blocking given its role in HIPAA (Health Information Portability and Accountability Act) enforcement, especially as it relates to consumer access under HIPAA's individual right of access.
- The Federal Trade Commission (**FTC**) may be involved in some information blocking activities, as actors may be subject to other FTC authorities should their actions related to information sharing be deemed anticompetitive. The FTC also has primary jurisdiction over consumer-facing applications, which may be involved in information blocking actions on behalf of consumers.

ADVANCING INFORMATION BLOCKING ENFORCEMENT TO FULFILL THE PROMISE OF INTEROPERABLE DATE EXCHANGE

Over the past several months, Leavitt Partners has convened and surveyed leading provider organizations, payers, health information networks, and consumer-facing applications to ascertain what changes are needed—in regulation, enforcement approach, and statute—to address some of the challenges that persist nine years after the passage of the Cures Act. Informed by the feedback from these stakeholders, we, Leavitt Partners, offer the below policy recommendations.

[9] 42 CFR § 1003.1400 et seq. — Civil monetary penalties for information blocking, as established by the U.S. Department of Health and Human Services Office of Inspector General, pursuant to the final rule published July 3, 2023 (88 FR 42982), effective September 1, 2023.

[10] 21st Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking, published as a Final Rule in the Federal Register on July 1, 2024, with regulations codified primarily at 42 CFR §§ 412.24, 495.4, 495.10, 511.2, 511.165, and 425.216, among others.

Increasing the Flow of Complaints

One of the major challenges for ASTP/ONC, OIG, and CMS in taking action against information blockers is the lack of complaints that are submitted. This can be attributed to several potential factors, including a lack of knowledge about the option to report, reticence by data exchange partners to report another entity, concern about how a report of information blocking may be construed by an actor with whom an entity shares patients or other business relationships, and others. We recommend that HHS collectively, with ASTP/ONC, OIG, CMS, and OCR as prime drivers to increase the prevalence of reporting through the following actions:

- **Educate**: Inform actors and consumers about their rights and options when they are denied access to their health information.
    - There should be a structured action plan from the agencies, including:
        - National training for health systems, vendors, and payers on requirements to share data, with a robust message that data sharing is the expectation, not the exception
        - Training on what allowable exceptions do exist
        - More robust communication about timelines and compliance requirements
- **Ensure Transparency**: While ASTP/ONC has created a useful dashboard for what complaints have been received, no public reporting of enforcement actions, violators, and compliance rates has occurred.[11] Full transparency about these figures would instill trust in consumers, provide real-world proof that submitting a claim would lead to change, and help the industry understand that the government is serious about data sharing.
- **Empower Patients**: ASTP/ONC, OCR, and CMS have made great strides to advance consumer engagement in their healthcare, encouraging patients to engage more broadly with applications, take control of their care, and engage more as consumers of healthcare. In this vein, HHS should create new and innovative tools to advance the ability of consumers to quickly elevate any denial of information or access to medical records to OCR for HIPAA enforcement and to ASTP/ONC for information blocking action.
- **Create Qui Tam-Like Authorization**: In other OIG enforcement contexts, specifically those related to the Anti-Kickback Statute (AKS) and the Physician Self-Referral Law (commonly known as the Stark Law) connected to the False Claims Act, individuals are authorized to pursue a cause of action against specific actors on behalf of the government. In those instances, when a CMP is levied against a violator, the individual who initiated the action may be given some of the payment.

[11] See: https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers

- If HHS/OIG is precluded from authorizing Qui Tam or Qui Tam-like functions, new protections for whistleblowers must be established. Individuals at many providers, networks, and developers may have specific knowledge about product development or internal practices that make it more difficult to share information. If incentives for disclosure are infeasible, safeguards for staff who report suspected information blocking are essential.

Info Blocking: Ideal Process

	**There should be only one knowledge standard and one penalty paradigm:**
	ONC/ASTP receives a complaint and refers it to OIG.
	OIG and ONC/ASTP determine if a regulated Actor knew or should have known their actions would lead to information blocking.
	If OIG finds information blocking, the Actor should be subject to civil monetary penalties.

Standardizing Penalties for Actors

Penalties for providers differ from those of other actors. As noted previously, providers are subject to appropriate disincentives (e.g., penalties in MIPS, the Merit-based Incentive Payment System) while other actors are subject to defined penalties (CMPs). This differentiation causes challenges for enforcement, including the involvement of additional agencies. For example, CMS must define appropriate disincentives and then enforce those penalties after OIG has made a finding of fault.

We believe that penalties should be standardized across all actors and be simplified to a uniform, CMP-based approach. We note that it would take an act of Congress to change the statutory definitions and requirements regarding information blocking penalties. However, we believe that this standardization and simplification is critical to creating an enforcement paradigm that is consistent, operationally achievable, and predictable for regulated actors.

In the absence of congressional action, HHS can still do much to provide certainty to regulated entities while advancing the data exchange that Congress expected when Cures was passed in 2016. Under current regulation, HHS has only defined “disincentives” for a subset of provider actors. While current regulations apply to a large number of provider entities in the country, they do not come close to capturing the majority of provider types. For example, labs, pharmacies, ambulance providers, skilled-nursing providers, long-term care facilities, community health centers, ambulatory surgical centers, and other entities have no identified disincentive.

This means that even if one of those providers was found to be in violation of the law, HHS would have no disincentive in place to apply to them. **HHS must continue with rulemaking for these additional entities.** We again note that congressional action to simplify the penalty paradigm would simplify enforcement and remove the need for additional rulemaking.

In addition to establishing disincentives for providers not currently subject to any penalties, HHS should amend its various regulations for providers and health IT vendors to require more default data-sharing functionality within their product offerings. Many EHRs already ship their products with auto-on data sharing within their workflows. HHS should consider requiring functionality within health IT that defaults such activity unless a valid exception is documented. Similarly, if a provider turns off default sharing enabled by their certified EHR technology or other data-sharing system (without a valid exception), and that significantly impedes the flow of information, the provider should be subject to penalties.

Last, while avoidance of information blocking is already a condition of certification of ONC/ASTP's Health IT Certification Program, ONC/ASTP could make it clearer to health IT developers that it is ready and willing to decertify the products of information blockers, if necessary. The threat of decertification can and should be another tool in ONC/ASTP's toolbox for enforcing information blocking requirements.

Knowledge Standards

When investigating a claim of information blocking, OIG is statutorily required to consider whether the actor had knowingly impeded the exchange of data or information as required. However, the Cures Act applies a different knowledge standard for networks and health IT vendors or developers.

For health IT developers and HIEs/HINs, the standard is whether they know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI. This knowledge standard provides for enforcement when an actor has actual knowledge that a process or technology is blocking the flow of information or constructive knowledge (i.e., they should know that what they are doing is likely to stop the flow of information). A provider, on the other hand, has only the "actual knowledge" standard.

Divergent knowledge standards create operational challenges that do not meaningfully advance public policy. Additionally, giving providers an actual knowledge standard allows for situations where a minimal amount of investigation would uncover information blocking issues but an incentive structure to be intentionally uninformed about data exchange practices. We recommend that Congress revise the knowledge standards and create a unified knowledge standard for all regulated entities. This standard should focus on both actual knowledge as well as constructive knowledge of practices that would impede the exchange of information. Organizations must accept accountability. Actors should not be "let off the hook" by intentionally putting their head in the sand. Blocking is blocking. If you aren't sharing, you should know better and do better. Intentional ignorance must not serve as a shield—failure to share data is information blocking, regardless of sophistication or setting.

Additional Enforcement Resources

One of the major enforcement challenges for OIG is the lack of dedicated funding for information blocking enforcement. Civil monetary penalties (CMPs) collected by OIG *may* be used to cover operating expenses but otherwise revert to Medicare trust funds, while any penalties levied pursuant to appropriate disincentives are kept by CMS. While HHS has the authority to fund information blocking enforcement at OIG through collected CMPs, HHS has thus far declined to do so. We recommend that Congress and/or HHS consistently fund OIG through one of two mechanisms:

- Annual Appropriations: Congress provides an annual appropriation to OIG to fund a number of activities, including the investigation of False Claims Act, Physician Self-Referral Act, and AKS actions.[12] We strongly recommend that OIG receive additional appropriations to staff at least five dedicated individuals that can investigate claims of information blocking.
- OIG Keeps a Portion of CMPs: HHS uses its authority to fund OIG through a portion of levied CMPs. While this could incentivize OIG to pursue claims against developers and networks over providers, allowing OIG to keep some portion of collected penalties would fund the organization in ways that limit new governmental spending and incent OIG to prioritize information blocking claims in addition to the other work it has to do.

In addition to consistent funding for OIG, we recommend that Congress give ASTP/ONC advisory opinion authority. While we appreciate the work that ASTP/ONC has done to advance the understanding of risks and responsibilities for actors as it relates to information blocking through FAQs and other advisories, we have heard from many regulated actors that these are insufficient. Absent binding advisory opinion authority that is also binding on OIG, many actors have indicated that they will not fully trust, and therefore cannot rely on, FAQs. This has led to organizations that should be sharing information to forgo sharing, believing that their exposure is limited and organizations seeking data with limited ability to point to binding guidance on what data holders must do.

What else is needed?

[12] See: https://www.hhs.gov/sites/default/files/fy-2026-oig-cj.pdf

SUMMARY OF RECOMMENDATIONS BY SECTOR

To clearly delineate the path forward, the following consolidates the paper's recommendations into a sector-specific road map. These actions—assigned to Congress, ONC/ASTP, OIG, CMS, and industry—are necessary to strengthen enforcement and ensure that information blocking prohibitions achieve their intended impact.

Congress

- Appropriate dedicated funding for OIG information blocking enforcement (e.g., at least five dedicated staff)
- Permit OIG to retain a portion of collected CMPs
- Harmonize penalties across all actors by creating a uniform CMP-based approach (replacing the current "appropriate disincentives" model for providers)
- Revise statutory knowledge standards to align all actors under a single standard that includes both actual and constructive knowledge
- Give ASTP/ONC statutory authority to issue binding advisory opinions on information blocking

ASTP / ONC

- Signal intent to decertify products under the Health IT Certification Program if developers of such products are found to commit information blocking
- Require certified health IT to include default on data-sharing functionality unless a valid exception is documented
- In coordination with CMS, continue rulemaking to extend disincentives to provider types not currently covered (e.g., labs, pharmacies, long-term care)

OIG

- Expand investigative capacity by adding dedicated staff and resources
- Enforce penalties consistently across developers, networks, and providers
- Coordinate with ONC to ensure complaints are acted upon quickly and transparently

CMS

- Define and implement "appropriate disincentives" for providers not currently subject to penalties
- Enforce penalties on providers referred by OIG, ensuring alignment with MIPS and other payment programs
- Collaborate with ONC to strengthen clarity and predictability in enforcement
- Explore creating and enforcing penalties for providers that disable EHR default data sharing that significantly impedes data sharing

Industry (Providers, Developers, Networks, Payers)

- Treat data sharing as the default expectation, rather than the exception
- Eliminate intentional ignorance of blocking rules; ensure compliance with both actual and constructive knowledge standards
- Implement systems and workflows that default to patient and provider access, with exceptions used only when legally justified
- Support transparency by reporting information blocking when observed and complying with enforcement mechanisms

CONCLUSION

Unless the current administration gets serious about enforcing information blocking requirements, with additional resources and clarifications, many healthcare stakeholders will continue to avoid data sharing in ways that were expected by Congress and required by law. Access to health data will continue to be delayed or denied, which will undermine care coordination, patient empowerment, and the interoperability infrastructure Congress envisioned. Regardless of other regulations or voluntary pledges, data will not flow across all sectors of the healthcare ecosystem as it should.

Without decisive action, the promise of a modern, interoperable health data infrastructure will remain out of reach, ultimately undermining efforts to advance value-based care, improve overall outcomes, and strengthen consumer trust. Conversely, stronger enforcement will not only curb harmful practices but will also accelerate innovation and enable more seamless care coordination, patient and consumer satisfaction, and reduced costs to the entire system. The choice is between a fragmented, inefficient status quo—or a care delivery system that delivers better outcomes for patients, providers, and communities alike.

ABOUT THE AUTHOR

Leavitt Partners, an HMA company, is a leading healthcare consulting firm that has consistently been at the forefront of navigating and advancing change in healthcare, including in digital health. Leavitt Partners achieves this through convening multisector alliances to address some of the most complex issues in healthcare; these groups include the CARIN Alliance, which since 2016 has worked to advance interoperability in health data.

ABOUT AVIA

The nation's leading digital transformation partner for 80+ healthcare organizations, empowering healthcare leaders with strategic insights, proven tools, and expert guidance to drive improved clinical outcomes, operational efficiencies, and financial performance. AVIA Network brings a collaborative approach to health systems with results-driven insights and innovative digital solutions to address pressing healthcare challenges with confidence.