ASTP Assistant Secretary for Technology Policy

Where are we and where do we go from here?

February 11, 2026

Disclaimers & Reminders

The contents of this presentation are based on cited references, including the provisions codified in 45 CFR part 171 and preamble discussion of these provisions in relevant final rules. While every effort has been made to ensure the accuracy of this presentation of those provisions, this presentation does not have the force of law. Statutes and regulations have the force of law. Therefore, in the event of any inconsistency between this presentation and any relevant statute or regulation, the statute or regulation controls.

Please note that other Federal, state or tribal laws may also apply.

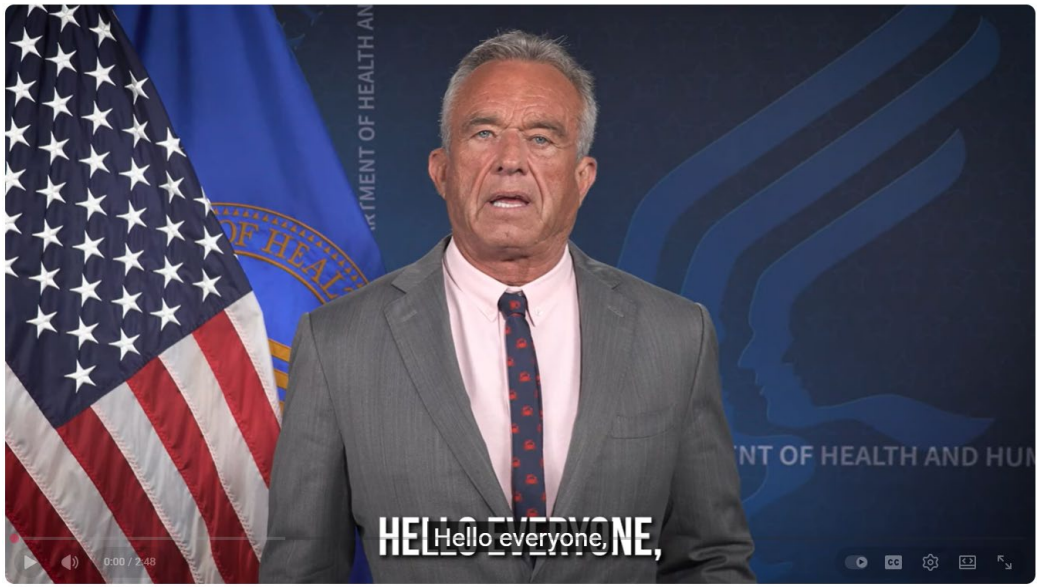
This communication is produced and disseminated at U.S. taxpayer expense.

The HTI-5: Deregulatory Actions to Unleash Prosperity Proposed Rule includes several proposed revisions to information blocking regulations.

- Find the rule and link to submit public comments at: https://www.federalregister.gov
- Public comment period closes Feb 27, 2026.

Check Tomorrow's Agenda for HTI-5 Breakout Session Details

HHS Secretary Kennedy Announces Expanded Enforcement of Information Blocking Regulations

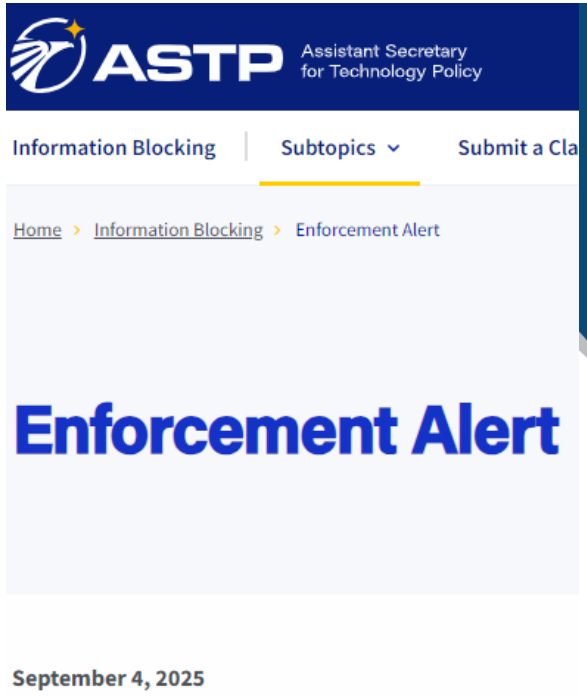


Secretary Kennedy Announces Expanded Enforcement of Health Care Information Blocking Regulations

"We will not tolerate any company that blocks your right to access your health information—or your right to share it with the trusted parties you choose.“
-Secretary Kennedy

https://www.youtube.com/watch?v=u1N7bX0cgvI&t=19s

Enforcement Alert – Information Blocking



ENFORCEMENT ALERT
Information Blocking

U.S. Department of Health and Human Services
Office of Inspector General
ASTP Assistant Secretary for Technology Policy

September 4, 2025

Stopping information blocking to unleash innovation and empower patients and their health care providers with friction-free information is a top priority for the Secretary of the Department of Health and Human Services and the Administration. The Office of Inspector General (OIG) and the Office of the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC) are issuing this enforcement alert to signal our joint commitment to intensify enforcement activity, dedicate additional resources, and take decisive action to detect and end information blocking.

The availability of electronic health information when and where it is needed is a critical element of a high-functioning health care system. Information blocking threatens patient care and undermines efforts by providers, payers, and others to make the health system more efficient and to improve quality of care. It puts at risk the substantial taxpayer investments made to encourage and support the adoption and use of technologies such as electronic health records.

What Is Information Blocking?

The 21st Century Cures Act (Cures Act) defines information blocking as a practice by an individual or entity that is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information except as required by law or as specified in an information blocking exception.

ASTP/ONC has issued regulations addressing information blocking, including identifying limited exceptions—such as to protect privacy or ensure security—where an entity will not be considered to have committed information blocking if its actions meet the conditions of the exceptions (45 CFR Part 171).

What Are the Consequences for Information Blockers?

Individuals and entities found to have engaged in information blocking may face several types of enforcement actions:

OIG Civil Monetary Penalties. OIG has a long history of investigating serious misconduct that impacts HHS programs and the people they serve. OIG has the authority to investigate claims of information blocking and impose civil monetary penalties (CMPs) against individuals and entities that commit information blocking (42 U.S.C. 300jj-52). Specifically, OIG may impose CMPs of **up to $1 million** per violation against:

- Health IT developers of certified health IT,
- Entities offering certified health IT,
- Health information exchanges (HIEs), and
- Health information networks (HINs).

OIG will prioritize enforcement where practices cause patient harm, significantly impact or impair a provider's ability to deliver patient care, are of long duration, or cause financial loss to Federal health care programs or other Government or private entities. Additional information about OIG's investigative process and OIG enforcement priorities may be found on OIG's information blocking page.

ASTP/ONC Certification Program Ban and/or Termination of Certification. ASTP/ONC can ban a developer of certified health IT that information blocks from the ONC Health IT Certification Program and may also terminate the certification of health IT involved in information blocking. ASTP/ONC intends to investigate and take swift action where warranted. Additional information can be found on ASTP/ONC's information blocking page.

ENFORCEMENT ALERT
Information Blocking

U.S. Department of Health and Human Services
Office of Inspector General
ASTP Assistant Secretary for Technology Policy

CMS Health Care Provider Disincentives. Under the Cures Act, OIG may investigate and refer providers that engage in information blocking to the Department, which may impose appropriate disincentives. CMS has established specific disincentives that it may apply to the following providers:

- Eligible hospitals and critical access hospitals participating in the Medicare Promoting Interoperability Program;
- Merit-based Incentive Payment System eligible clinicians (including a group practice); and
- A Medicare Shared Savings Program accountable care organization (ACO), ACO participants, and ACO providers/suppliers.

More information about CMS information blocking disincentives is found in the final rule.

The Department is committed to using all available authorities to hold information blockers accountable and prevent future violations. OIG and ASTP/ONC are coordinating closely with each other and with other Department partners.

How to Avoid Information Blocking

Voluntary compliance now can prevent serious consequences later. Stopping information blocking protects patients and strengthens the health care system. If you or your organization are engaged in practices that could constitute information blocking, now is the time to bring those practices into compliance. The statutory and regulatory framework is in place, and enforcement is active. More information on compliance with information blocking may be found here:

- ASTP/ONC's information blocking page
- OIG's information blocking page

How to Report Suspected Information Blocking

If you believe you are the victim of information blocking, are aware of information blocking practices, or have seen them happen, your voice matters. Sharing your experience can help protect patients, improve care, and strengthen our health system for everyone. We want to hear from you.

The preferred way to report is through ASTP/ONC's Information Blocking Portal. Complaints reported through the portal are shared with OIG. Reports may also be submitted online through the OIG Hotline or by calling 1-800-HHS-TIPS (1-800-447-8477).

When submitting a report:

- Please provide as much detail as you can about the suspected information blocking. Health care or IT expertise is not needed to submit a report.
- **You may submit reports anonymously**, though providing your contact information can help us follow up and better understand the situation.
- Your identity and the details you share are legally protected, including from disclosure under the Freedom of Information Act. OIG and ASTP/ONC will protect your identity to the extent permitted by law.

Your story can make a difference!

Each report may help stop harmful practices, supports fair access to information, and ensures that the health care system works for the people it is meant to serve.

Interagency Coordination: Public Health Service Act – 300jj-52

(c) Identifying barriers to exchange of certified health information technology […]

(3) Referral The National Coordinator and the Office for Civil Rights of the Department of Health and Human Services may refer to the Inspector General instances or patterns of refusal to exchange health information with an individual or entity using certified electronic health record technology that is technically capable of trusted exchange and under conditions when exchange is legally permissible.

(d) Additional provisions

(1) Information sharing provisions The National Coordinator may serve as a technical consultant to the Inspector General and the Federal Trade Commission for purposes of carrying out this section.
The National Coordinator may, notwithstanding any other provision of law, share information related to claims or investigations under subsection (b) with the Federal Trade Commission for purposes of such investigations and shall share information with the Inspector General, as required by law.

FTC Expresses Unanimous Support for ONC Cures Act Final Rule

Third Party Submitting IB Claim – New – June 2025

Can I have a third party submit an information blocking claim on my behalf?

Yes. Anyone, individually or as a group, can have a third party of their choosing submit a claim of possible information blocking to HHS on their behalf.

ID:IB.FAQ52.1.2025JUN

https://healthit.gov/faq/can-i-have-a-third-party-submit-an-information-blocking-claim-on-my-behalf/

Interference FAQ – New – July 2025

Would it be considered an interference under the information blocking regulations if a health IT developer of certified health IT limited a customer's or a user's choice of QHINs for the purposes of participating in TEFCA?

Yes, it would likely be considered an interference with the access, exchange, or use of EHI if an actor restricts or impedes a customer or user from obtaining or using the QHIN connectivity services of their choice because such services provide for the access, exchange, and use of EHI.

The information blocking law (42 U.S.C. § 300jj-52) may be implicated when an actor engages in exclusionary, discriminatory, or other practices that impede the dissemination or use of interoperable technologies and services, and that interfere with the access, exchange, or use of EHI (85 FR 25813-25814). Examples of practices by a developer of certified health IT that would likely be an interference include practices that restrict or impede a customer's or a user's access, exchange, or use of EHI through QHIN connectivity services by: establishing contractual terms that limit or have the effect of reducing the choices of a customer or user to use any QHIN; imposing unreasonable fees for access to certain QHINs; and taking unnecessary time for configuration changes or other technical steps needed to use a QHIN's connectivity services. Each of these examples would be especially concerning when the QHIN may be a competitor of the actor because it may indicate that different fee structures or terms do not reflect genuine differences in the cost or the effort required to provide access, exchange, or use of EHI (85 FR 25814, 85 FR 25881-25882; 45 CFR 170.302(a)(2)).

ID:IB.FAQ53.2025JUL

FAQ on automation technologies – New – December 2025

Could an actor's practice that interferes with an automation technology's ability to access, exchange, or use EHI implicate the information blocking regulations?

Yes. An actor's practice that interferes with, prevents, or materially discourages the access, exchange, or use of EHI by automation technologies (e.g., robotic process automation (RPA), agentic artificial intelligence) could implicate the information blocking regulations. The information blocking definition (42 CFR 171.103) is not specific to any particular means, manners, or mechanisms by which access, exchange, or use of EHI is sought and could be accomplished. Thus, an actor's practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI by automation technologies could implicate the information blocking provision.

ID:IB.FAQ54.2025DEC

https://www.healthit.gov/faq/could-actors-practice-interferes-automation-technologys-ability-access-exchange-or-use-ehi

Manner Exception FAQ – 1 of 2 New – December 2025

Does an actor have to provide all the EHI requested by a requestor to satisfy the Manner Exception?

Generally, yes, but it may depend on the circumstances.

The scope of EHI[1] for which the actor must fulfill a request for access, exchange, or use in order to satisfy the Manner Exception is determined by the scope of the *request* and thus by the requestor. This is true regardless of whether the actor seeks to fulfill the request consistent with the *manner requested* condition (*see* 45 CFR 171.301(a)), the *alternative manner* condition (45 CFR 171.301(b)), or a combination of the conditions.

If the requestor's request is for access, exchange, or use of a subset of EHI that the actor can fulfill in the manner requested (45 CFR 171.301(a)), then the actor can satisfy the Manner Exception by providing access, exchange, or use of that subset of EHI in that requestor-specified manner so long as the actor's practice in doing so is otherwise consistent with the Manner Exception (45 CFR 171.301).

By contrast, if the actor cannot reach an agreement with the requestor or is not technically capable of providing all of the requested EHI in a particular requestor-specified manner, then to satisfy the Manner Exception for the request the actor would need to use one or more additional alternative manners specified by the requestor (45 CFR 171.301(b)(1)(i) and (ii)) or agreed to by the requestor (45 CFR 171.301(b)(1)(iii)), working through manners in the priority order identified in the *alternative manner* condition, until the actor has made all requested EHI available to the requestor.

An actor might have the technical capability to satisfy the Manner Exception for only some of the EHI requested in the manner(s) the requestor specifies. In such instances, the actor may want to consider whether another exception may apply for the remaining EHI not fulfilled through the Manner Exception.

[1] EHI is defined for purposes of the information blocking regulations in 45 CFR 171.102. On and after October 6, 2022, the scope of EHI for purposes of the information blocking definition (45 CFR 171.103) is EHI as defined in 45 CFR 171.102 (89 FR 1199, 85 FR 70069).

ID:IB.FAQ55.2025DEC

Manner Exception FAQ – 2 of 2 New – December 2025

What role does a "requestor" play under the alternative manner condition of the Manner Exception?

When an actor believes they can fulfill a request for access, exchange, or use of electronic health information (EHI), they may seek to satisfy the Manner Exception (45 CFR 171.301) to be sure they are not committing information blocking. The Manner Exception states in principle that an actor "must fulfill a request for EHI in any manner requested, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested" (45 CFR 171.301(a)(1), 85 FR 25877). If an actor does not fulfill a request for EHI in any manner requested because the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor, the Manner Exception then specifies that an actor must fulfill the request in an *alternative manner* (45 CFR 171.301(b)).

Under this *alternative manner* condition of the Manner Exception, the actor must fulfill the request for EHI without unnecessary delay in an alternative manner (45 CFR 171.301(b), 85 FR 25878). The actor must offer alternative manners in a strict priority order, starting with 45 CFR 171.301(b)(1)(i) and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in the paragraph.

Importantly, a requestor must specify the technology or standards, respectively, of the alternative manners under paragraphs (b)(1)(i) and (ii) or agree to an alternative machine-readable format under paragraph (b)(1(iii). Simply put, if the requestor does not specify technology certified to a standard or standards adopted in part 170 ((b)(1)(i)), or content and transport standards published by certain publishers ((b)(1)(ii)), or agree to an alternative machine-readable format ((b)(1)(iii)), then the actor cannot meet the *alternative manner* condition of the Manner Exception. An actor is not permitted to presume or dictate the manner in which access, exchange, or use of EHI is fulfilled under the *alternative manner* condition of the Manner Exception.

If an actor is unable to meet the Manner Exception, the actor may want to consider whether the actor can meet the conditions of another exception. For example, the actor may be able to rely on the Infeasibility Exception. One factor of the *infeasible under the circumstances* condition of the Infeasibility Exception is "why the actor was unable to provide access, exchange, or use of electronic health information consistent with the Manner Exception." (45 CFR 171.204(a)(5)(i)(F), 85 FR 25867).

ID:IB.FAQ56.2025DEC

Fees Exception FAQ – New – December 2025

Can an actor meet the Fees Exception if it conditions the access, exchange, or use of EHI on the establishment of a revenue sharing agreement?

No. For an actor's practice of charging fees for access, exchange, or use of EHI to not be considered information blocking under the Fees Exception, the fees an actor charges must not be based on the revenue that the requestor derives or may derive from the access, exchange, or use of the EHI (45 CFR 171.302(a)(2)(ii)). The conditioning of access, exchange, or use of EHI on the establishment of "revenue sharing" or "royalty agreements" with third parties seeking access, exchange, or use of EHI provided by an actor to a requestor that go beyond recovering costs reasonably incurred by the actor to enable the access, exchange, or use of EHI could implicate the information blocking provision (85 FR 25882, 85 FR 25879).

ID:IB.FAQ57.2025DEC

Goals of the HTI-5 Proposed Rule

The HTI-5 Proposed Rule has three core goals:

1. Reducing burden on health IT developers by streamlining the ONC Health IT Certification Program (Certification Program) by removing redundant requirements;

2. Updating the information blocking regulations to better promote EHI access, exchange, and use so that patients' access to their data is not blocked; and

3. Advancing a new foundation of Fast Healthcare Interoperability Resources (FHIR®)-based application programming interfaces (APIs) that promote AI-enabled interoperability solutions through modernized standards and certification.

Cost Savings:

- $1.53 billion, including $650 million over the next 5 years for health IT developers, providers, and other stakeholders.

- The proposed revisions and removal of certification criteria from the Certification Program are estimated to save certified health IT developers more than 1.4 million compliance hours in their first year (an average savings of 4,000 hours per developer) – giving developers new capacity to deliver innovative solutions for their customers.

- The proposed deregulatory actions reduce the effort of developers of certified health IT to meet ongoing Certification Program requirements and reduce barriers to entry for new Certification Program participants.

Current Definitions - § 171.102

Proposal:

Revise the “access” and “use” definitions in § 171.102 to emphasize that the definitions include automated means of access, exchange, or use of EHI — including, without limitation, autonomous AI systems.

Additional “Alternative” Proposal:

In addition to updating the “access” and “use” definitions, potentially similarly revise the “exchange” definition.

Infeasibility Exception - § 171.204

Third party seeking modification use condition - § 171.204(a)(3)

Proposal: Remove.

Manner exception exhausted condition - § 171.204(a)(4)

Proposal: Revise to:

- Require all three “alternative” manners from the Manner Exception alternative manner condition be offered

- Replace “[t]he actor does not provide the same access, exchange, or use of the requested electronic health information to a substantial number of individuals or entities that are similarly situated to the requestor”

  with

  “[t]he actor does not provide analogous access, exchange, or use of the requested electronic health information to any other individual or entity”

  - Essentially, we are proposing to replace “same” with “analogous” and remove the “substantial number” and “similarly situated” conditions.

Alternative Proposal: Remove the condition.

Manner Exception - § 171.301
Manner requested condition - § 171.301(a)

Proposal:

Add text explicitly stating that ***any contract or agreement*** under which the actor and requestor agree to fulfill a request for access, exchange, or use of EHI, and any license from the actor of interoperability elements used in fulfilling the request in the manner requested:

- Must be at market rate;
- Must not be a contract of adhesion; or
- Must not contain unconscionable terms.

Add definitions to § 171.102 for market rate, contract of adhesion, and unconscionable terms

Alternative Proposal:

- Remove paragraph (a)(2) from the *manner requested* condition of the Manner Exception (excludes application of the Fees and Licensing Exceptions to agreements under paragraph (a) to fulfill requests for EHI in any manner requested.
- Apply the conditions of both the Fees Exception and Licensing Exception to any agreement an actor makes with a requestor related to fulfilling the request for access, exchange, or use of EHI in any manner requested.

Whether or Not a Proposal is Adopted

- The *manner requested* condition only covers the technical manner of exchange of the requested EHI.
- Contracts or agreements for access, exchange, and use of EHI cannot be contracts of adhesion or contracts containing unconscionable terms. These types of contracts are not covered by the Manner Exception even if these agreements were styled as, or in fact were, achieving access, exchange, or use of the requested EHI in the requested manner. These types of contracts would also likely constitute an interference under the information blocking regulations. (90 FR 61012)

Trusted Exchange Framework and Common Agreement (TEFCA) Manner Exception - § 171.403

Proposal:

Remove the TEFCA Manner Exception (§ 171.403) and associated definitions.

COMMENT PERIOD

Dec. 29, 2025 – Feb. 27, 2026.

URL: HealthIT.gov/Proposedrule

Regulatory Definition of “Interfere With” or “Interference” (§ 171.102)

***Interference* means “to prevent, materially discourage, or otherwise inhibit.”**

- Mirrors the statutory language referring to practices “likely to interfere with, prevent, or materially discourage” access, exchange, or use of EHI.

Previous Proposal to Codify Descriptions of Interference Practices

HTI-2 Proposed Rule

- ONC proposed to codify specific practices in § 171.104 that constitute interference
- Codified list is not exhaustive—other practices may constitute interference based on circumstances.
- Specific practices are not referred to as examples (due to intent-based nature of statute)
- This proposal was withdrawn, along with others not yet finalized from HTI-2 Proposed Rule, December 29, 2025.

Description of Interference:

Actions That Impose Delays on Access, Exchange, or Use of EHI

- Actions taken by an actor to impose delays on another person's ability to access, exchange, or use EHI constitute an interference.
- Includes both affirmative acts and omissions designed or structured to slow data movement.
- Delays are a common category of interference raised through FAQs, reports, and stakeholder inquiries.

Description of Interference:

Delaying Access for Patient-Authorized Apps Using APIs

- Delaying the **access, exchange, or use of EHI** by a **third-party app designated and authorized by the patient** constitutes an interference **when a deployed API is capable** of supporting that access.

- "App" includes patient-facing smartphones, web apps, wearables, and other tools leveraging modern APIs (e.g., § 170.315(g)(10)-certified APIs).

- Directly tied to ONC's Cures Act mandate to ensure **seamless patient access via APIs**.

- One of the strongest examples of interference because delays undermine the statutory right of patients to access their EHI where APIs are operational.

Description of Interference:

Failure to Publish Required API Technical Information

- Failure to publish or make available essential API-related details—such as **service base URLs for Certified API Technology**—is an **interference**

- These omissions prevent apps, developers, and other systems from connecting or requesting EHI as intended under the Cures Act.

Description of Interference:

Non-Standard or other Inappropriate Implementations of Health IT

- Implementing health IT in **non-standard ways that limit interoperability** or complicate how others access, exchange, or use EHI is an interference. Includes proprietary configurations, custom interfaces, or restrictions that frustrate standardized data exchange.

- Implementing health IT in ways that **lead to fraud, waste, or abuse, or impede innovations and advancements** in health information access, exchange, and use, including care delivery enabled by health IT

Description of Interference:

Improper Inducements or Discriminatory Contract Terms

- Contractual conditions that **discriminate among persons and entities** seeking access, exchange, or use of EHI may constitute interferences.

- Includes leveraging contracts to impose unequal terms, unnecessary conditions, or burdens unrelated to legitimate privacy/security requirements.

Public Health Service Act: 3001(c)(5)(D)

(D) CONDITIONS OF CERTIFICATION — […] the Secretary, through notice and comment rulemaking, shall require, as a condition of certification and maintenance of certification…that the health information technology developer or entity—

(i) does not take any action that **constitutes information blocking** as defined in section 3022(a);

(ii) provides **assurances** satisfactory to the Secretary that such developer or entity, unless for legitimate purposes specified by the Secretary, will not take any action described in clause (i) or any other action that may inhibit the appropriate exchange, access, and use of electronic health information; […]

(iv) has **published application programming interfaces** and allows health information from such technology to be accessed, exchanged, and used without special effort through the use of application programming interfaces or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws

Conditions and Maintenance of Certification Requirements

The 21st Century Cures Act requires HHS to establish Conditions and Maintenance of Certification requirements for the ONC Health IT Certification Program.

Seven (7) Conditions of Certification with Maintenance of Certification Requirements
• Information Blocking
• Assurances
• Communications
• Application Programming Interfaces (APIs)
• Real World Testing
• Attestations
• Insights (EHR Reporting Program)

ONC Certification Program Oversight: Direct Review

§ 170.580 ONC review of certified health IT

(a) ***Direct Review*** […]

(2)[…](iii) ***Noncompliance with a Condition and Maintenance of Certification requirement.*** ONC may initiate direct review under this section if it has a reasonable belief that a health IT developer has not complied with a Condition or Maintenance of Certification requirement under subpart D of this part. […]

(4) ***Coordination with the Office of Inspector General.*** […]

(b) ***Notice*** […] (2) ***Notice of non-conformity*** —

(i) ***Circumstances that may trigger notice of non-conformity.*** At any time during its review of certified health IT or a health IT developer's actions or practices under paragraph (a) of this section, ONC may send a notice of non-conformity to the health IT developer if it determines that certified health IT or a health IT developer's actions or practices does not conform to the requirements of the ONC Health IT Certification Program

(f) ***Termination*** — (1) ***Applicability.*** The National Coordinator may terminate a certification if:[…]

(iii) A determination is made that the health IT developer is noncompliant with a Condition or Maintenance of Certification requirement under subpart D of this part

§ 170.581 Certification ban.

(a) ***Circumstances that may trigger a certification ban.*** The certification of any of a health IT developer's health IT is prohibited when: […]

(2) ONC determines a certification ban is appropriate per its review under § 170.580(a)(2)(iii).

Report Information Blocking Portal Page

Information Blocking Portal

WHAT IS THE STATUS OF MY REPORT?

Report Information Blocking

Additional Considerations:

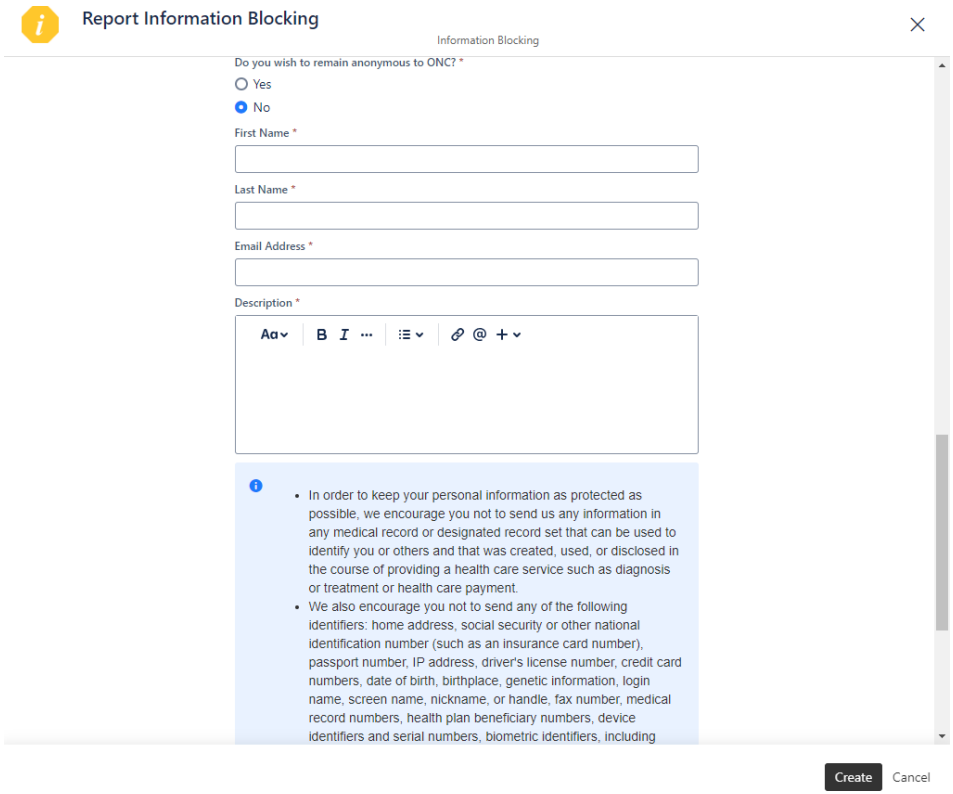
- If you believe that a HIPAA covered entity or business associate violated your (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy, Security or Breach Notification Rules, please file your complaint directly with The HHS Office for Civil Rights
- By law, information received by ONC in connection with a claim or suggestion of possible information blocking that could identity who submitted the claim is exempt from mandatory disclosure under the Freedom of Information Act.

You are NOT required to submit any personally identifying information when submitting concerns, complaints, feedback, or inquires. If you want to remain anonymous to ONC, please click the "yes" button within the submission window.

In order to keep your personal information as protected as possible, we encourage you not to send us any information in any medical record or designated record set that can be used to identify you or others and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment or health care payment.

We also encourage you not to send ONC any of the following identifiers: home address, social security or other national identification number (such as an insurance card number), passport number, IP address, driver's license number, credit card numbers, date of birth, birthplace, genetic information, login name, screen name, nickname, or handle, fax number, medical record numbers, health plan beneficiary numbers, device identifiers and serial numbers, biometric identifiers, including finger and voice prints, and full face photographic images and any comparable images (such as a MRI or x-rays).

Report Information Blocking Portal (direct link):
https://healthit.gov/report-info-blocking



Where to Find More Information

ASTP Website Resources

- Information Blocking Webpage (Fact Sheets, FAQs, Blogs, Webinars & Presentations, Press/Media): https://www.healthit.gov/topic/information-blocking
- Information Blocking FAQs: https://www.healthit.gov/topic/information-blocking
- Health IT Buzz Blog: https://www.healthit.gov/buzz-blog/
- ASTP Speaker Request Form: https://www.healthit.gov/speaker-request-form

Reach out via phone or web

202-690-7151

Feedback & Questions: https://www.healthit.gov/feedback

Report Information Blocking Portal (direct link): https://healthit.gov/report-info-blocking

ASTP Speaker Request Form: https://www.healthit.gov/speaker-request-form

Stay connected, follow us on socials

@HHS_TechPolicy

Assistant Secretary for Technology Policy

www.youtube.com/@HHS_TechPolicy

Subscribe to our weekly eblast at healthit.gov for the latest updates!

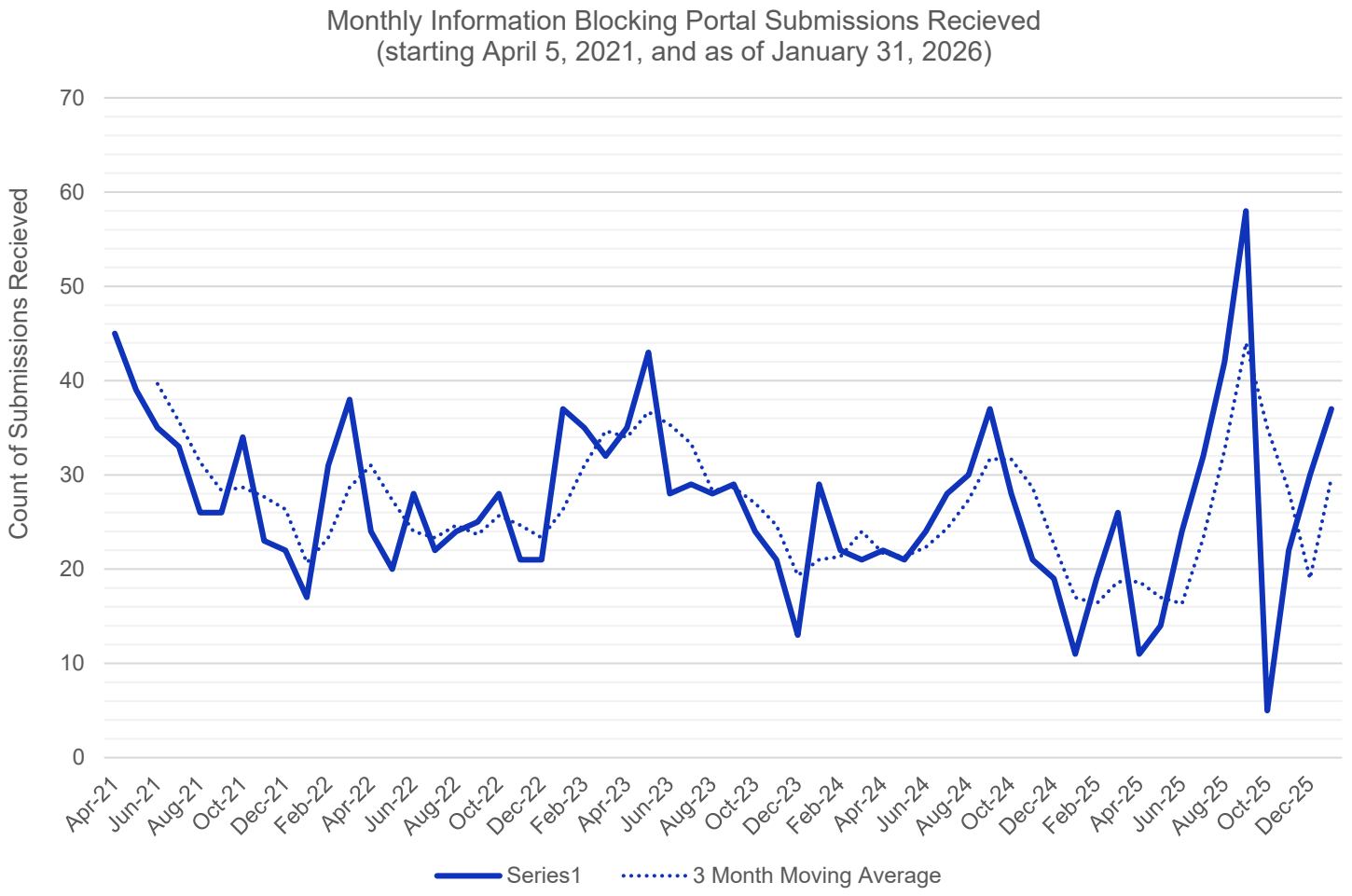
ASTP Assistant Secretary for Technology Policy

IB Claims Data and HIO/Hospital IB Survey Results

February 11, 2025

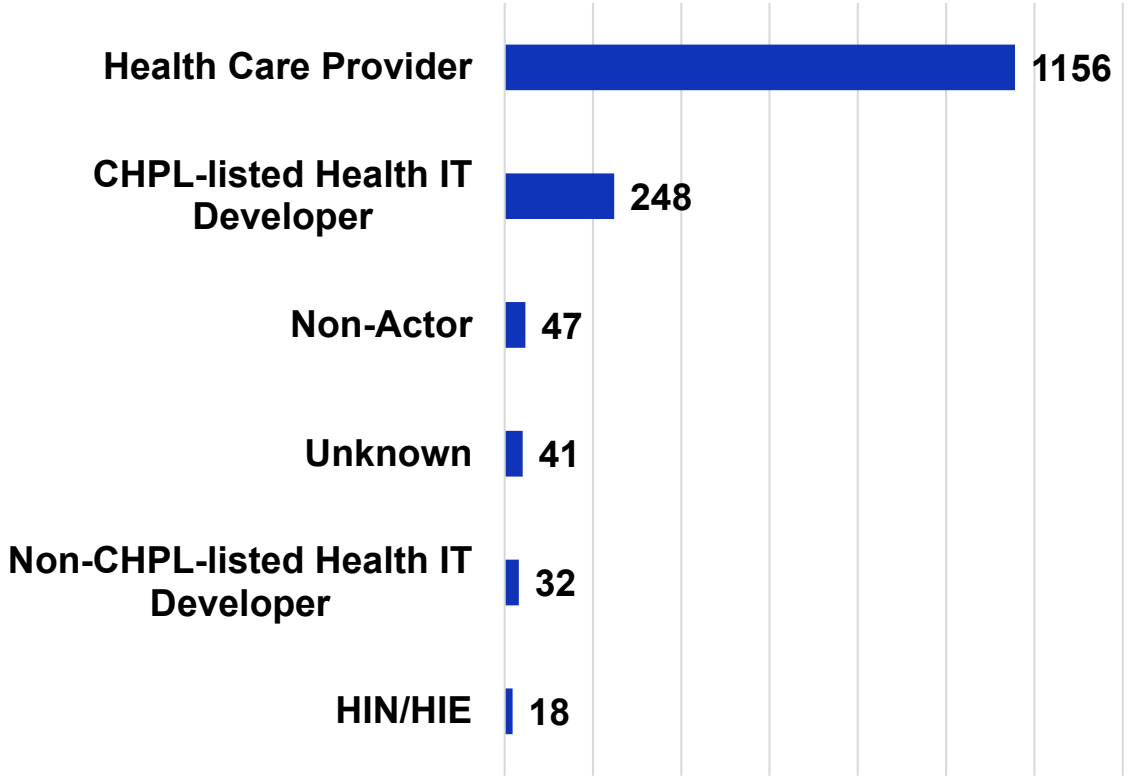
Information Blocking Claims Received by ASTP: Summary Counts

Summary counts as of 1/31/2026	
Total number of information blocking portal submissions received	1,572
Total number of possible claims of information blocking	1,483
Total number of submissions received that did not appear to be claims of potential information blocking	89

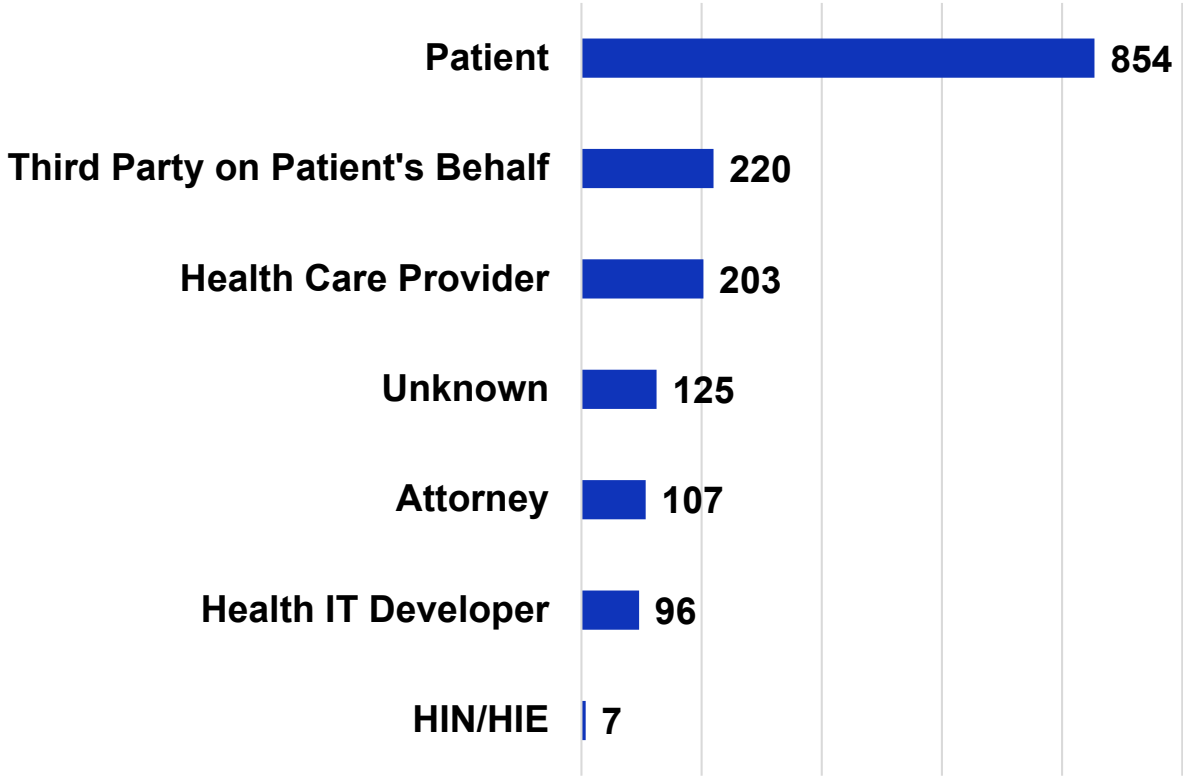


Information Blocking Claims Received by ASTP: Summary Counts

Claims Counts by Potential Actor



Claims Counts by Type of Claimant



*Numbers current as of 1/31/2026

Disclaimers on Information Blocking Claims Counts

- The distribution of claims of possible information blocking received by ASTP through the Report Information Blocking Portal is not likely to be completely representative of the totality of possible information blocking that is occurring.
  - In national survey data presented by ONC, 92% of responding HIOs and 97% of responding hospitals said they “Never/Rarely” report potential information blocking to HHS.
  - Entities may be reluctant to submit claims of possible information blocking to HHS due to concerns about possible retaliation by the subject of their claim. By law, information received by ONC in connection with a claim or suggestion of possible information blocking that could identity who submitted the claim is exempt from mandatory disclosure under the Freedom of Information Act.

- Information on categorization of claims is based solely on ASTP’s inference from the facts and allegations as presented by the claimant.

- Any determination as to whether an information blocking actor’s conduct met the information blocking definition or not would require a fact-based, case-by-case investigation and review against all elements of the information blocking definition.

Information Blocking Quick Stats: Information Blocking Claims by the Numbers

Report Information Blocking Portal Page

Information Blocking Portal

WHAT IS THE STATUS OF MY REPORT?

Report Information Blocking

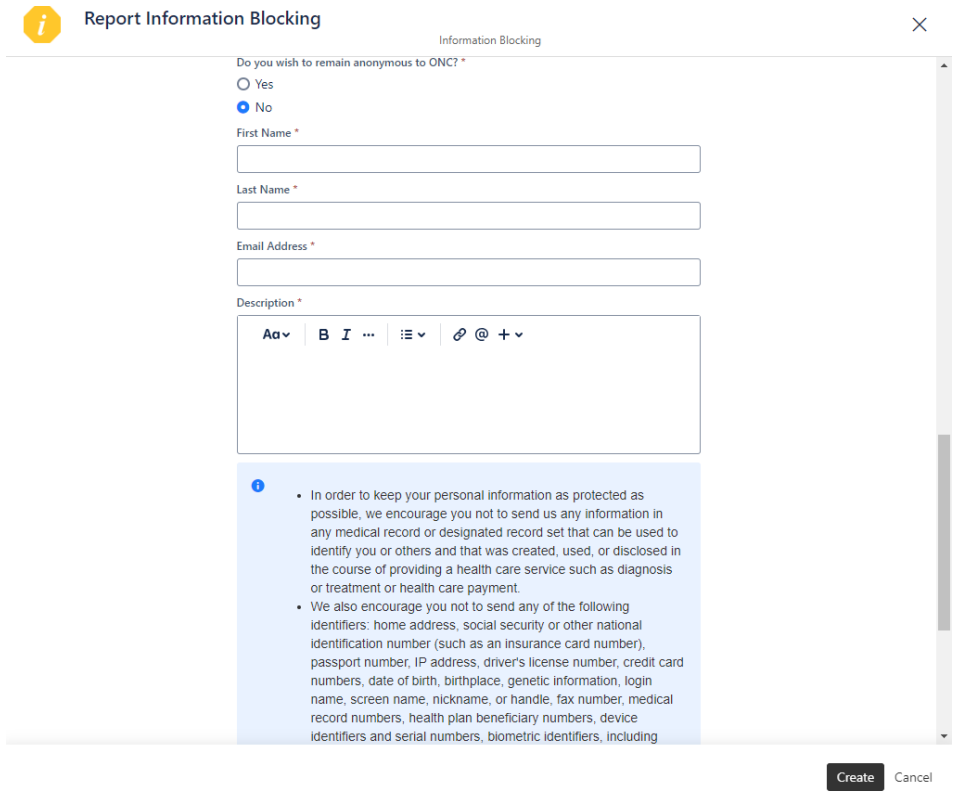
Additional Considerations:

- If you believe that a HIPAA covered entity or business associate violated your (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy, Security or Breach Notification Rules, please file your complaint directly with The HHS Office for Civil Rights
- By law, information received by ONC in connection with a claim or suggestion of possible information blocking that could identity who submitted the claim is exempt from mandatory disclosure under the Freedom of Information Act.

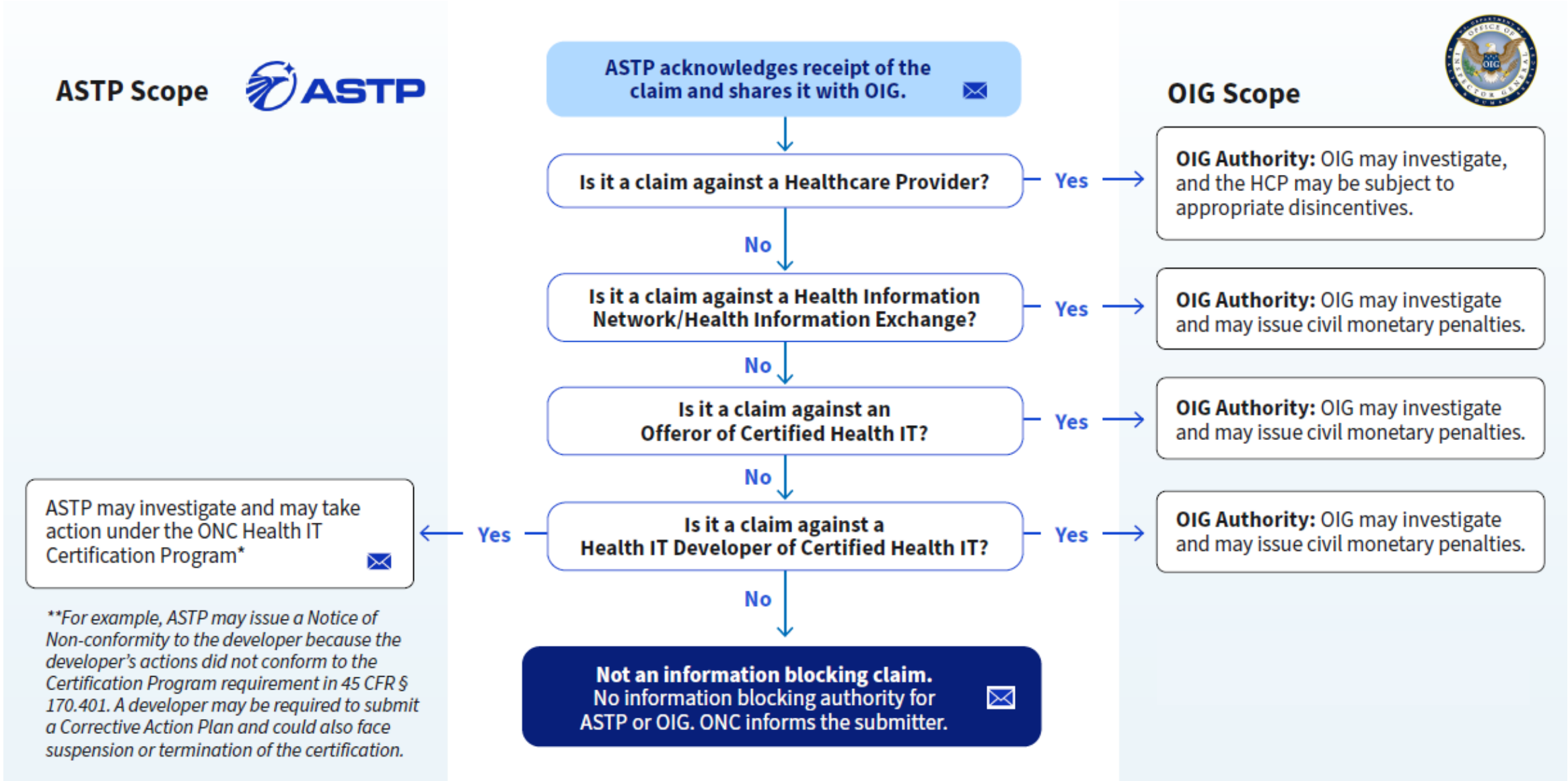
You are NOT required to submit any personally identifying information when submitting concerns, complaints, feedback, or inquires. If you want to remain anonymous to ONC, please click the "yes" button within the submission window.

In order to keep your personal information as protected as possible, we encourage you not to send us any information in any medical record or designated record set that can be used to identify you or others and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment or health care payment.

We also encourage you not to send ONC any of the following identifiers: home address, social security or other national identification number (such as an insurance card number), passport number, IP address, driver's license number, credit card numbers, date of birth, birthplace, genetic information, login name, screen name, nickname, or handle, fax number, medical record numbers, health plan beneficiary numbers, device identifiers and serial numbers, biometric identifiers, including finger and voice prints, and full face photographic images and any comparable images (such as a MRI or x-rays).



Information Blocking Portal Process – Overview

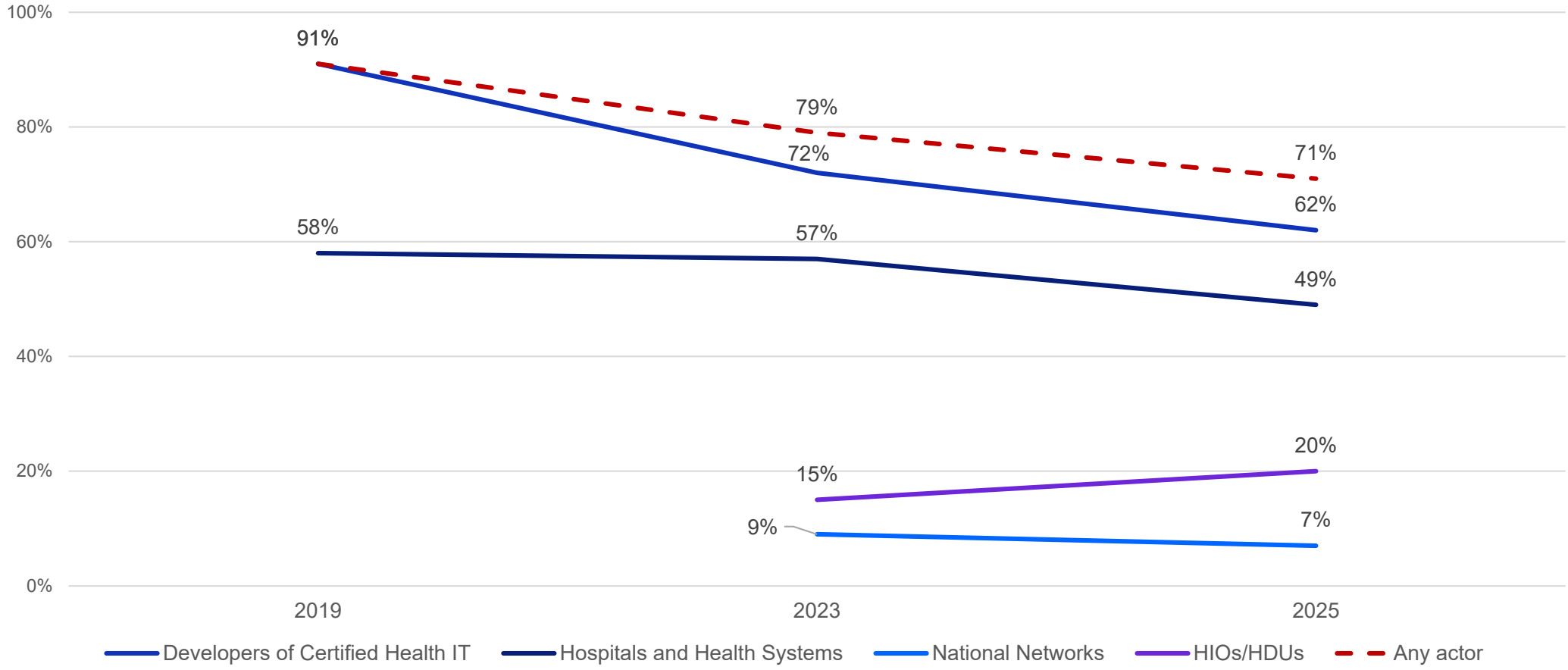


Health Information Exchange Organizations (HIOs/HDUs)

Experiences of Perceived Information Blocking from a National Survey

The percentage of HIOs reporting potential information blocking across any actor decreased from 2019 to 2025.

Percent of HIOs that reported an entity sometimes or routinely engaged in potential information blocking, 2019-2025.



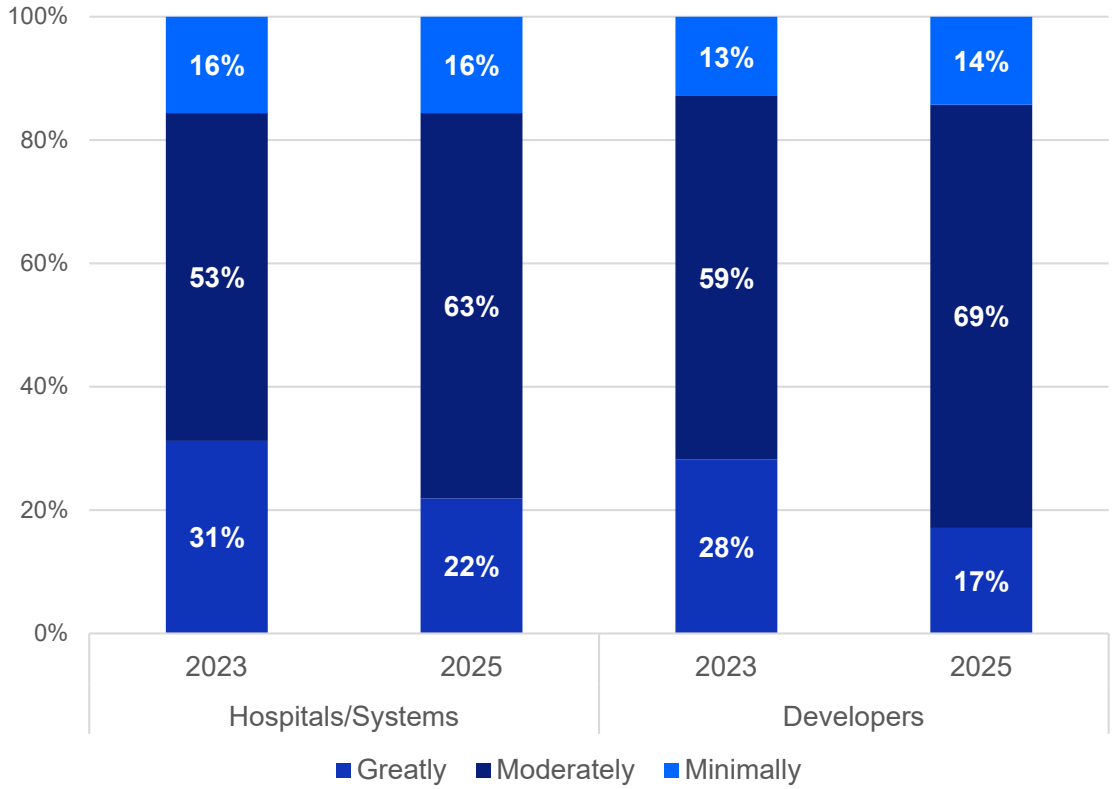
Source: National Survey of Health Information Organizations: 2019, 2023 and 2025.

Most HIOs reported that potential information blocking has either a great or moderate impact on information exchange.

Percent of HIOs that reported developers and hospitals sometimes or routinely used types of practices they perceived as potential information blocking.

Potential Information Blocking Practice	2019	2023	2025
Developer of Certified Health IT			
Price, unreasonable fees	81%	60%	59%
Artificial barriers	65%	49%	40%
Contract language	51%	43%	30%
Refusal	52%	32%	27%
Hospitals and Health Systems			
Strategic affiliations	--	45%	42%
Artificial barriers	34%	25%	22%
Refusal	52%	40%	31%

Percent of HIOs who reported that experiencing potential information blocking affected their services.



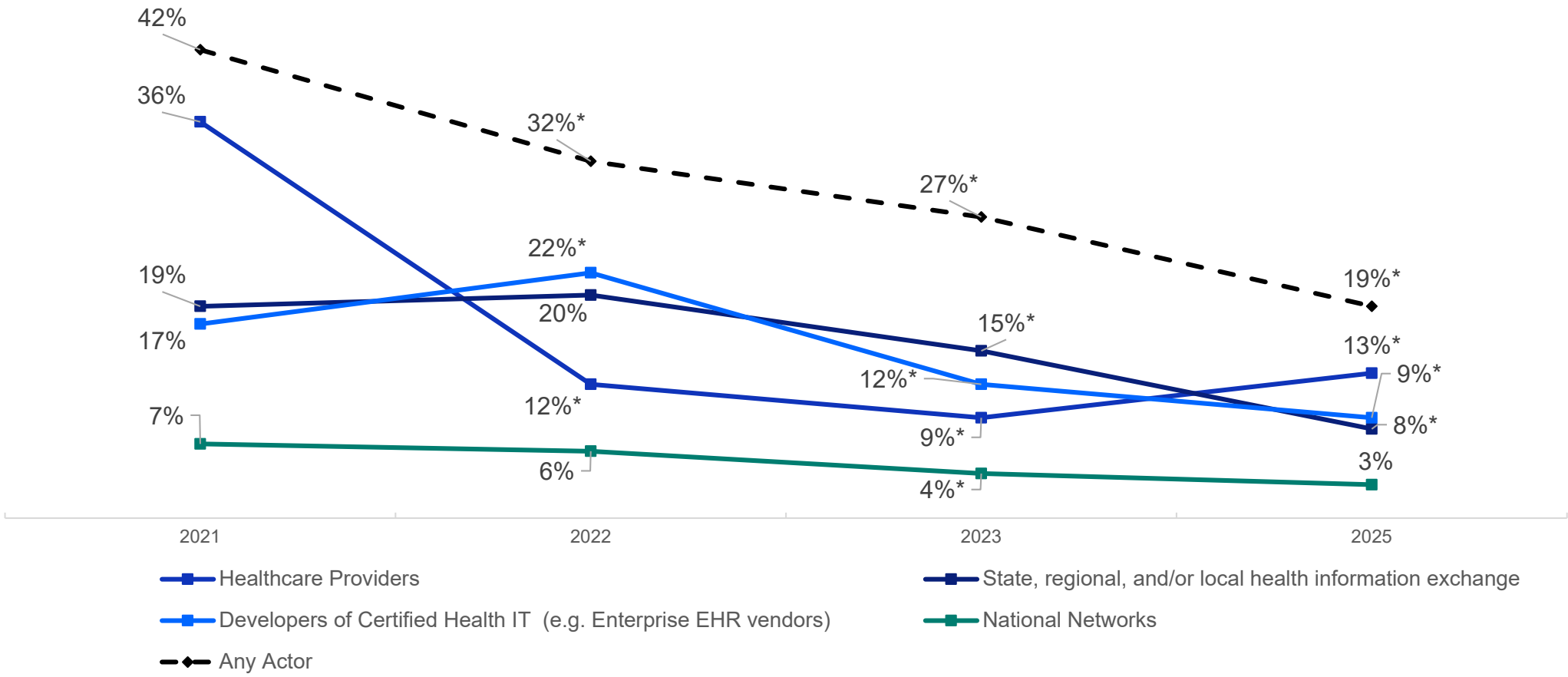
Source: National Survey of Health Information Organizations, 2019, 2023 and 2025.

Hospitals

Experiences of Perceived Information Blocking from a National Survey

The percentage of hospitals reporting potential information blocking across any actor decreased from 2021 to 2025.

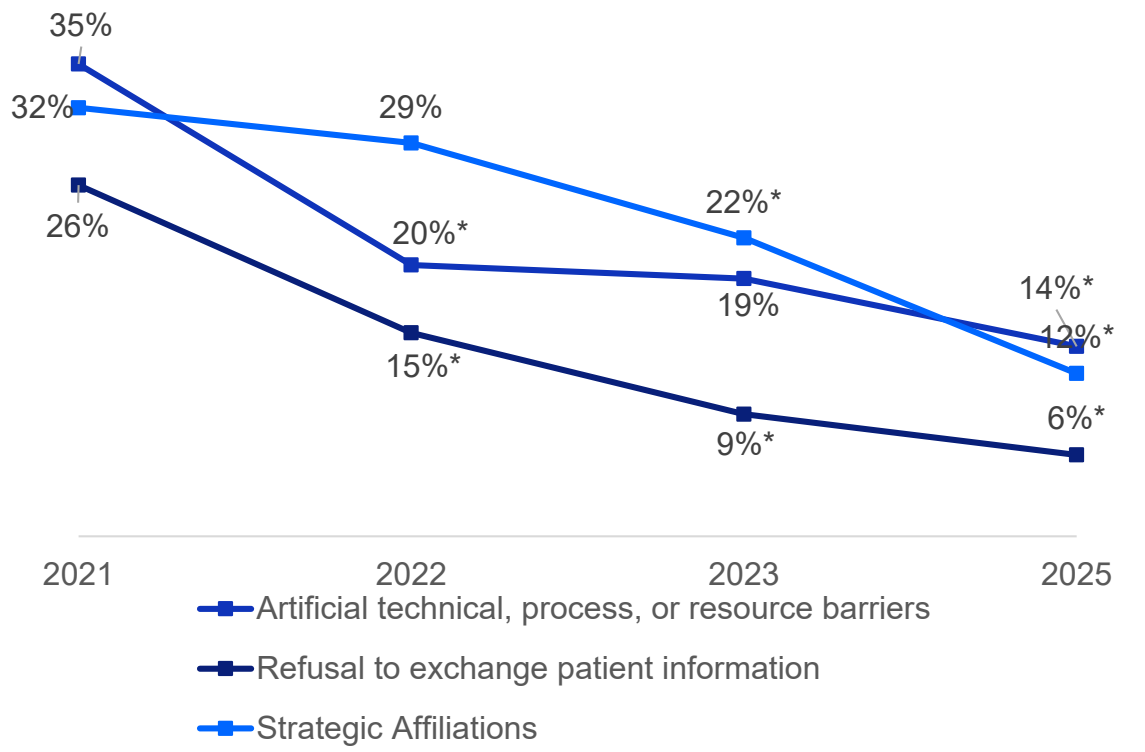
Percent of hospitals that reported an entity sometimes or routinely engaged in potential information blocking, 2021-2025.



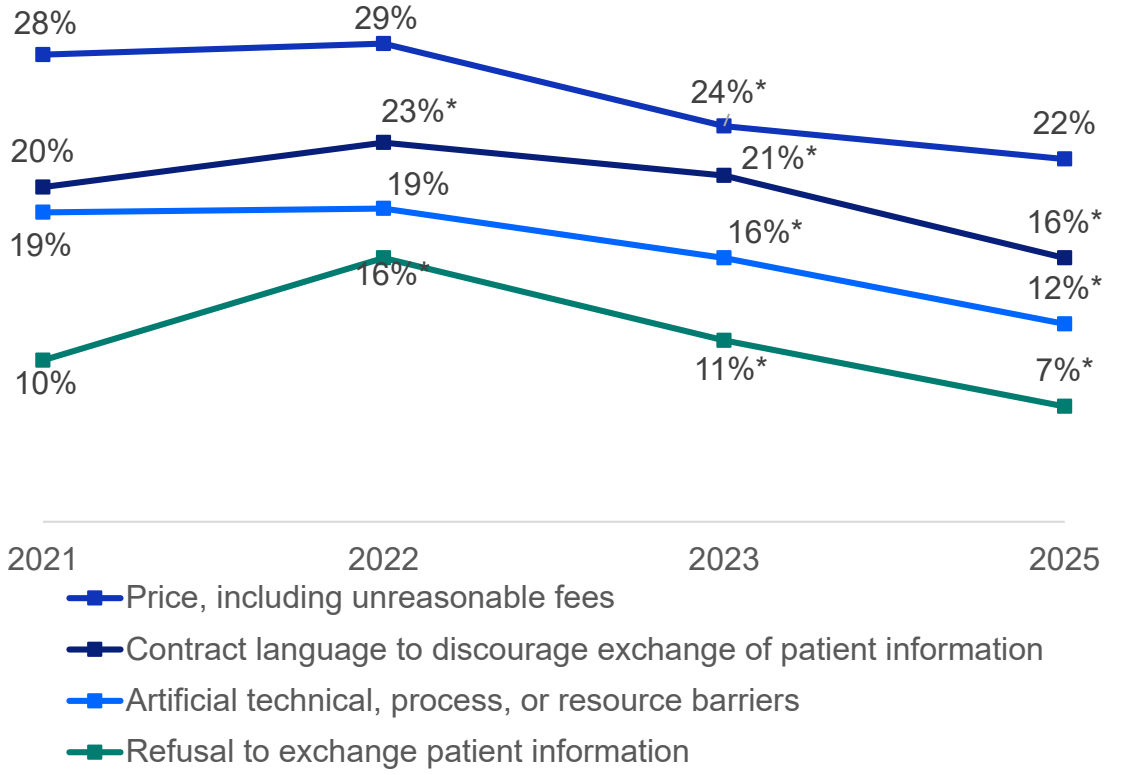
Source: American Hospital Association Information Technology Survey, 2021-2025.

All types of information blocking declined from 2021 to 2025, but certain forms remained common

Percent of Hospitals that Perceived Healthcare Providers Engaged in Three Types of Information Blocking



Percent of Hospitals that Perceived EHR Developers Engaged in Four Types of Information Blocking



Source: American Hospital Association Information Technology Survey, 2021-2025.

Where to Find More Information

ASTP Website Resources

- Information Blocking Webpage (Fact Sheets, FAQs, Blogs, Webinars & Presentations, Press/Media): https://www.healthit.gov/topic/information-blocking
- Information Blocking FAQs: https://www.healthit.gov/topic/information-blocking
- Health IT Buzz Blog: https://www.healthit.gov/buzz-blog/
- ASTP Speaker Request Form: https://www.healthit.gov/speaker-request-form

Reach out via phone or web

202-690-7151

Feedback & Questions: https://www.healthit.gov/feedback

Report Information Blocking Portal (direct link): https://healthit.gov/report-info-blocking

ASTP Speaker Request Form: https://www.healthit.gov/speaker-request-form

Stay connected, follow us on socials

@HHS_TechPolicy

Assistant Secretary for Technology Policy

www.youtube.com/@HHS_TechPolicy

Subscribe to our weekly eblast at healthit.gov for the latest updates!

ASTP Assistant Secretary for Technology Policy

Preventing Harm Exception

February 11, 2026

Disclaimers

- **The contents of this presentation are based on the provisions codified in 45 CFR part 171 and preamble discussion of these provisions in relevant final rules.** While every effort has been made to ensure the accuracy of this presentation of those provisions, this presentation is not a legal document. Statutes and regulations have the force of law. Therefore, in the event of any inconsistency between this presentation and any relevant statute or regulation, the statute or regulation controls.

- Please note that other Federal, state or tribal laws may also apply.

- This communication is produced and disseminated at U.S. taxpayer expense.

⚠ Information blocking exceptions do not override an actor's obligation to comply with a mandate in another federal, state, or (where applicable) tribal law, enforceable in court, to make health information available.

⚠ The information blocking statute is separate from HIPAA. Information blocking regulations and the HIPAA Privacy, Security, and Breach Notification Rules operate separately and on the basis of their independent statutory authorities.

⚠ An actor that is also required to comply with the HIPAA Privacy Rule must comply with the individual right of access as codified in 45 CFR 164.524 regardless of whether the actor may be able to satisfy an exception to the "information blocking" definition with respect to some or all of the PHI they may have for any given individual.

Reminder: Information Blocking Exceptions Are Voluntary

- Each information blocking exception is voluntary, and is designed and intended to offer certainty that practices that meet the exception's conditions will not be considered “information blocking.”
- An actor’s practice (act or omission) that does not meet the conditions of an exception will not automatically constitute information blocking. Instead, such practices will be evaluated on a case-by-case basis to determine whether information blocking has occurred.

Elements of the Information Blocking Definition

To be "Information Blocking," a practice (act or omission) must:

- ❑Not be required by law;
- ❑Be done by actor regulated under the information blocking statute;
- ❑Involve electronic health information (EHI);
- ❑Be done with requisite knowledge by the actor; and
- ❑Be likely to interfere with access, exchange, or use of EHI;
- ❑Not be covered by an exception.

Interfere with or *interference* means to prevent, materially discourage, or otherwise inhibit.

Information Blocking Exceptions in Effect Today

Exceptions that involve not fulfilling requests to access, exchange, or use EHI

1. Preventing Harm Exception

2. Privacy Exception

3. Security Exception

4. Infeasibility Exception

5. Health IT Performance Exception

6. Protecting Care Access Exception

Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

7. Manner Exception

8. Fees Exception

9. Licensing Exception

Exceptions that involve practices related to actors' participation in TEFCA

10. TEFCA Manner Exception

The Preventing Harm Exception – § 171.201

§ 171.201 Preventing harm exception—when will an actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking?

An actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when the practice meets the conditions in paragraphs (a) and (b) of this section, satisfies at least one condition from each of paragraphs (c), (d), and (f) of this section, and also meets the condition in paragraph (e) of this section when applicable.

The Preventing Harm Exception – § 171.201

Paragraphs (a) and (b) – must always be met in their entirety for exception to cover a practice

(a) Reasonable belief. The actor engaging in the practice must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information affected by the practice. For purposes of this section, "patient" means a natural person who is the subject of the electronic health information affected by the practice.

(b) *Practice breadth.* The practice must be no broader than necessary to substantially reduce the risk of harm that the practice is implemented to reduce.

The Preventing Harm Exception – § 171.201

Paragraph (c) – a practice must satisfy one of these *type of risk* conditions for the exception to apply

(c) ***Type of risk.*** The risk of harm must:

(1) Be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose electronic health information is affected by the determination;

or

(2) Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

The Preventing Harm Exception – § 171.201

Paragraph (d) – which *type of harm* must be met turns on the *type of risk;* and where the risk is determined on individualized basis on who is seeking whose information

(d) ***Type of harm.*** The type of harm must be one that could serve as grounds for a covered entity (as defined in § 160.103 of this title) to deny access (as the term "access" is used in part 164 of this title) to an individual's protected health information under:

(1) Section 164.524(a)(3)(iii) of this title where the practice is likely to, or in fact does, interfere with access, exchange, or use (as these terms are defined in § 171.102) of the patient's electronic health information by their legal representative (including but not limited to personal representatives recognized pursuant to 45 CFR 164.502) and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;

(2) Section 164.524(a)(3)(ii) of this title where the practice is likely to, or in fact does, interfere with the patient's or their legal representative's access to, use or exchange (as these terms are defined in § 171.102) of information that references another natural person and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;

(3) Section 164.524(a)(3)(i) of this title where the practice is likely to, or in fact does, interfere with the patient's access, exchange, or use (as these terms are defined in § 171.102) of their own electronic health information, regardless of whether the risk of harm that the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (2) of this section; or

(4) Section 164.524(a)(3)(i) of this title where the practice is likely to, or in fact does, interfere with a legally permissible access, exchange, or use (as these terms are defined in § 171.102) of electronic health information not described in paragraph (d)(1), (2), or (3) of this section, and regardless of whether the risk of harm the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (2) of this section.

The Preventing Harm Exception – § 171.201

Paragraph (e) – applies and must be met when the *type of risk* is determined on individualized basis

(e) ***Patient right to request review of individualized determination of risk of harm.*** Where the risk of harm is consistent with paragraph (c)(1) of this section, the actor must implement the practice in a manner consistent with any rights the individual patient whose electronic health information is affected may have under § 164.524(a)(4) of this title, or any Federal, State, or tribal law, to have the determination reviewed and potentially reversed.

The Preventing Harm Exception – § 171.201

Paragraph (f) – a practice must satisfy one of these conditions for exception to apply

(f) ***Practice implemented based on an organizational policy or a determination specific to the facts and circumstances.*** The practice must be consistent with an organizational policy that meets paragraph (f)(1) of this section or, in the absence of an organizational policy applicable to the practice or to its use in particular circumstances, the practice must be based on a determination that meets paragraph (f)(2) of this section.

(1) An organizational policy must:

(i) Be in writing;

(ii) Be based on relevant clinical, technical, and other appropriate expertise;

(iii) Be implemented in a consistent and non-discriminatory manner; and

(iv) Conform each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use.

(2) A determination must:

(i) Be based on facts and circumstances known or reasonably believed by the actor at the time the determination was made and while the practice remains in use; and

(ii) Be based on expertise relevant to implementing the practice consistent with the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use in particular circumstances.

Using the Preventing Harm Exception

Question:

My ICU patient dies while their spouse is not at the hospital with them. In my professional judgment, it is reasonably likely that patient's spouse will suffer substantial psychological or emotional harm from first learning via a portal or app that their spouse has died. Can the Preventing Harm Exception cover delaying availability of patient death information in the portal or API until I or a fellow clinician can break the news to them in real time?

Preventing Harm Exception:

- Where *type of risk* is **individually determined**, the actor must meet six conditions:
  - *Reasonable belief*;
  - *Practice breadth;*
  - *Type of risk;*
  - *Type of Harm;*
  - *Practice implemented based on an organizational policy or a determination specific to the facts and circumstances;*

  &
  - *Patient right to request review of individualized determination of risk of harm.*

*"Practices" will be evaluated on a case-by-case basis to determine whether information blocking has occurred. A practice likely to be an interference may not be information blocking if the actor's practice is required by law, satisfies the conditions of an exception, or is done without the knowledge required on the part of the actor by the information blocking definition.

Additional Resources:

- ONC's Information Blocking FAQs on HealthIT.gov

This scenario was presented 2/2/2022, "What Healthcare Providers Need to Know…" *(Webinar 3)*

Recording & Slide deck links available at: https://healthit.gov/information-blocking/#webinars-presentations

FAQ: In which patient access cases does the Preventing Harm Exception recognize "substantial harm" ?

The Preventing Harm Exception at 45 CFR 171.201 relies on the same types of harm as apply for a covered entity to deny access to protected health information under the HIPAA Privacy Rule (see 45 CFR 164.524(a)(3)). Where an actor's practice, based on an individualized (45 CFR 171.201(c)(1)) determination of risk, is likely to interfere with a patient's or patient representative's access, exchange, or use of the patient's EHI, the type of harm (45 CFR 171.201(d)) needed for the exception to apply depends on who is seeking access to the EHI, and what EHI they are seeking to access.[4]

The table below shows the *type of harm* recognized under the Preventing Harm Exception for several commonly encountered patient access scenarios.[1]

Access, exchange, or use of patient's EHI	EHI for which access, exchange, or use is affected by the interfering practice is	Applicable type of harm[1]	Regulation Text References
Patient exercising own right of access	Patient's EHI	Danger to life or physical safety of the patient or another person	§ 171.201(d)(3), referencing HIPAA Privacy Rule § 164.524(a)(3)(i)
	Patient's EHI that references another person	Substantial harm[3] to such other person	§ 171.201(d)(2), referencing HIPAA Privacy Rule § 164.524(a)(3)(ii)
Patient's personal representative as defined in HIPAA Privacy Rule (45 CFR 164.502) exercising right of access to patient's EHI *(for example, parent of a minor child)*[2]	Patient's EHI	Substantial harm[3] to the patient or to another person	§ 171.201(d)(1), referencing HIPAA Privacy Rule § 164.524(a)(3)(iii)
	Patient's EHI that references another person	Substantial harm[3] to such other person	§ 171.201(d)(2), referencing HIPAA Privacy Rule § 45 CFR 164.524(a)(3)(ii)

Notes:

1 - For simplicity of presentation, this table focuses only on patient access use case examples where risk has been determined on an individual basis (45 CFR 171.201(c)(1)). Where the risk arises from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (45 CFR 171.201(c)(2)), the exception's applicable type of harm conditions (45 CFR 171.201(d)(3) and (4)) recognize only danger to life or physical safety of the patient or another person.

2 - For more information about the definition of a "personal representative" under the HIPAA Privacy Rule, please see https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html

3 - "Substantial harm" includes "substantial physical, emotional, or psychological harm" (see, for example, *HIPAA Privacy Rule preamble at 65 FR 82556).*

4 - In order for the Preventing Harm Exception to cover any practice likely to interfere with access, exchange, or use of EHI based on an individualized (45 CFR 171.201(c)(1)) determination of risk, the practice must also satisfy requirements in 45 CFR 171.201(a), (b), (e), and (f).

https://www.healthit.gov/faq/which-patient-access-cases-does-preventing-harm-exception-recognize-substantial-harm

ID:IB.FAQ42.1.2022FEB

FAQ: Do the Preventing Harm Exception requirements for the type of harm align with the HIPAA Rules?

Yes. The Preventing Harm Exception's *type of harm* condition relies on the same types of harm that serve as grounds for reviewable denial of an individual's right of access under the Privacy Rule (45 CFR 164.524). (*See* ONC Cures Act Final Rule preamble Table 3—Mapping of Circumstances Under § 171.201(d) to Applicable Harm Standards.)

In most instances, including where a practice interferes with a patient's own or the patient's other health care providers' legally permissible access, exchange, or use of the patient's electronic health information (EHI), coverage under the Preventing Harm Exception requires that the risk be of physical harm. (*See* 45 CFR 171.201(d)(3) and (4).)

However, the Preventing Harm Exception's *type of harm* condition applies a "substantial harm" standard for practices interfering with a patient's ***representative's*** requested access, exchange, or use of the patient's EHI and to the patient's or their representative's access to other persons' individually identifiable information within the patient's EHI in some circumstances. (*See* 45 CFR 171.201(d)(1) and (2)).

ID:IB.FAQ32.1.2021JAN https://www.healthit.gov/faq/do-preventing-harm-exception-requirements-type-harm-align-hipaa-rules

FAQ: Will the Preventing Harm Exception cover practices interfering with a patient's access, exchange, or use of their EHI only for the purposes of reducing an imminent or immediate risk of harm?

No. The *reasonable belief* condition does not include a requirement that the harm be expected to occur within a particular time period or that the likelihood of the harm be high enough to be considered "imminent." (*See* 45 CFR 171.201(a)). The Preventing Harm Exception's *reasonable belief* condition requires an actor engaging in a practice likely to interfere with a patient's access, exchange, or use of their own EHI to have a reasonable belief that the practice will substantially reduce a risk to life or physical safety of the patient or another person that would otherwise arise from the affected access, exchange, or use.

https://www.healthit.gov/faq/will-preventing-harm-exception-cover-practices-interfering-patients-access-exchange-or-use ID:IB.FAQ34.1.2021JAN

FAQ: Would the Preventing Harm Exception cover a “blanket” several day delay on the release of laboratory or other test results to patients so an ordering clinician can evaluate each result for potential risk of harm associated with the release?

No. Blanket delays that affect a broad array of routine results do not qualify for the Preventing Harm Exception. The Preventing Harm Exception is designed to cover only those practices that are no broader than necessary to reduce a risk of harm to the patient or another person.

As we discussed in the Cures Act Final Rule, a clinician generally orders tests in the context of a clinician-patient relationship. In the context of that relationship, the clinician ordering a particular test would know the range of results that could be returned and could prospectively formulate, in the exercise of their professional judgment, an individualized determination for the specific patient that:

- withholding the results of the particular test(s) from the patient would substantially reduce a risk to the patient’s or another person’s life or physical safety

- or –

- that withholding the results of the particular test(s) from a representative of the patient would substantially reduce a risk of substantial harm to the patient or another person.

Such individualized determinations made in good faith by an ordering clinician, in the exercise of their professional judgment and in the context of the treatment relationship within which they order the test, would satisfy the *type of risk* and *type of harm* conditions of the Preventing Harm Exception. Actors, including but not limited to the ordering clinician, could implement practices in reliance on such determinations and the Preventing Harm Exception would cover such practices so long as the practices also satisfy the other four conditions of the exception.

https://www.healthit.gov/faq/would-preventing-harm-exception-cover-blanket-several-day-delay-release-laboratory-or-other

ID:IB.FAQ33.1.2021JAN

FAQ: Where the patient is a minor and to avoid breaching the patient's confidentiality and trust with the provider, will the Preventing Harm Exception cover an actor's practices that interfere with a parent or legal representative's access, exchange, or use of the minor's EHI?

No. Unless an actor reasonably believes a practice that interferes with a parent or other legal representative's requested access, exchange, or use of the minor's electronic health information (EHI) will substantially reduce a risk of at least substantial harm to the patient or another person, the **Preventing Harm Exception** is not designed to cover that practice.

The **Privacy Exception** contains a sub-exception (45 CFR 171.202(e)) that covers practices respecting an individual's request not to share information, subject to certain conditions.

https://healthit.gov/faq/where-patient-minor-and-avoid-breaching-patients-confidentiality-and-trust-provider-will/

ID:IB.FAQ31.1.2021JAN

FAQ: Where the patient is a minor and to reduce a risk of harm other than physical abuse, will the Preventing Harm Exception cover an actor's practices that interfere with a parent or legal guardian's access, exchange, or use of the minor's EHI?

Yes, where the *risk of harm* has been determined on an individualized basis and all other conditions of the Preventing Harm Exception are met. For example, the practice must be no broader than necessary and the actor must reasonably believe the practice will substantially reduce the risk of harm. (For all the conditions of the Preventing Harm Exception, please see **45 CFR 171.201**.)

For purposes of the Preventing Harm Exception, a parent or legal guardian would be considered a patient's legal representative. The Preventing Harm Exception's *type of harm* condition applies a "substantial harm" standard for practices interfering with a patient's ***representative's*** requested access, exchange, or use of the patient's EHI. (*See* 45 CFR 171.201(d)(1)).

The *type of harm* conditions for Preventing Harm Exception coverage of practices interfering with patients' and their representatives' access to EHI on the basis of an individualized determination of risk are specifically aligned with the HIPAA Privacy Rule's grounds for reviewable denial of an individual's right of access under the Privacy Rule. (*See also* ONC Cures Act Final Rule preamble **discussion** and **Table 3—Mapping of Circumstances Under § 171.201(d) to Applicable Harm Standards**).

https://healthit.gov/faq/where-patient-minor-and-reduce-risk-harm-other-physical-abuse-will-preventing-harm-exception/

IB.FAQ35.1.2021JAN

Where to Find More Information

ASTP Website Resources

- Information Blocking Webpage (Fact Sheets, FAQs, Blogs, Webinars & Presentations, Press/Media): https://www.healthit.gov/topic/information-blocking
- Information Blocking FAQs: https://www.healthit.gov/faqs
- Health IT Buzz Blog: https://www.healthit.gov/buzz-blog/
- ASTP Speaker Request Form: https://www.healthit.gov/speaker-request-form

Reach out via phone or web

202-690-7151

Feedback & Questions: https://www.healthit.gov/feedback

Report Information Blocking Portal (direct link): https://healthit.gov/report-info-blocking

ASTP Speaker Request Form: https://www.healthit.gov/speaker-request-form

Stay connected, follow us on socials

@HHS_TechPolicy

Assistant Secretary for Technology Policy

www.youtube.com/@HHS_TechPolicy

Subscribe to our weekly eblast at healthit.gov for the latest updates!

Information Blocking “Office Hours”

Submit your IB questions to us – tell us what you’d like to know and how ASTP/ONC can support IB education and enforcement!

Feedback & Questions: https://www.healthit.gov/feedback

Report Information Blocking Portal (direct link):
https://healthit.gov/report-info-blocking

20 ANNUAL 26 MEETING

@HHS_TechPolicy

Share your content on X and don't forget to use the hashtag #ASTP2026