ASTP Assistant Secretary for Technology Policy

Information Blocking 101 Review

February 11, 2026

Disclaimers & Reminders

This presentation is based on 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 its accuracy, 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

The Information Blocking Definition

45 CFR 171.103 Information blocking

(a) Information blocking means a practice that except as required by law or covered by an exception set forth in subparts B, C, or D of [45 CFR part 171], is likely to interfere with access, exchange, or use of electronic health information; and

(b) If conducted by:

(1) A health IT developer of certified health IT, health information network or health information exchange, such developer, network or exchange knows, or should know, that such practice is likely to interfere with access, exchange, or use of electronic health information; or

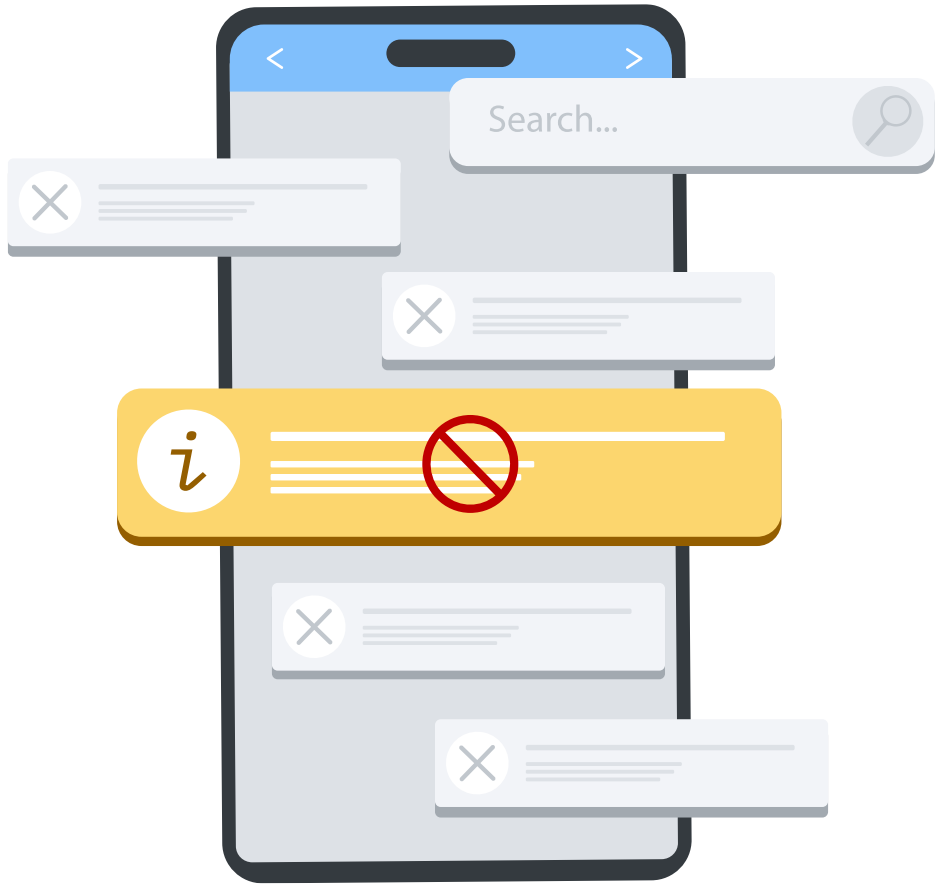
(2) A health care provider, such provider knows that such practice is unreasonable and is likely to interfere with access, exchange, or use of electronic health information.

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

Elements of the Information Blocking Definition

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

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



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

Required by Law

What does it mean for implementation purposes?

- Includes interferences with access, exchange, or use of EHI that are explicitly required by state or federal law.
- Distinguishes between interferences that are “required by law” and those engaged in pursuant to a privacy law, but which are not “required by law.”

Further Clarification from the 2020 Final Rule Preamble

- Federal and state law includes:

  Statutes, regulations, court orders, and binding administrative decisions or settlements, such as (at the Federal level) those from the FTC or the Equal Employment Opportunity Commission (EEOC)

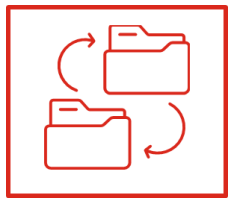
- Tribal laws, as applicable

Information Blocking Actors

Information blocking prohibition applies to three types of “actors”

Health Care Providers

Health IT Developers of Certified Health IT



Health Information Networks (HINs) & Health Information Exchanges (HIEs)

Each actor – individual or organization – is uniquely accountable for their own information blocking conduct

These terms are defined for purposes of the information blocking regulations in 45 CFR 171.102

Information Blocking Actors: Health Care Providers

Health care provider has the same meaning as ‘‘health care provider’’ in 42 U.S.C. 300jj.

Under this definition, “health care provider” includes a:

- Hospital
- Skilled nursing facility
- Nursing facility
- Home health entity or other long term care facility
- Health care clinic
- Community mental health center
- Renal dialysis facility,
- Blood center, Ambulatory surgical center
- Emergency medical services provider,
- Federally qualified health center
- Group practice
- Pharmacist
- Pharmacy
- Laboratory
- Physician
- Practitioner
- Provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization
- Rural health clinic
- Covered entity under section 256b of this title
- Ambulatory surgical center
- Therapist
- Any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary

Information Blocking Actors: Health IT Developers of Certified Health IT

Health IT developer of certified health IT means an individual or entity, other than a health care provider that self-develops health IT that is not offered to others, that **develops or offers** health information technology (as that term is defined in 42 U.S.C. 300jj(5)), and which has, **at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified** under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj-11(c)(5) (ONC Health IT Certification Program).

Information Blocking Actors: Health Information Networks & Exchanges (HINs/HIEs)

Health information network or health information exchange means an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information:

(1) Among **more than two unaffiliated individuals or entities** (other than the individual or entity to which this definition might apply) **that are enabled to exchange with each other**; and

(2) That is for a **treatment, payment, or health care operations** purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164.

What is **Electronic Health Information**?

"Electronic Health Information (EHI)" means **electronic protected health information (ePHI)** to the extent that the ePHI would be included in a **designated record set** as these terms are defined for HIPAA.

- Except for psychotherapy notes (45 CFR 164.501) and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- This is applicable whether or not the information is held by or for a HIPAA covered entity.

You can find the EHI definition in 45 CFR 171.102

What Is The **Requisite Knowledge**?

Health Care Providers

"…**knows** that such practice is **unreasonable** and is likely to interfere with the access, exchange or use of electronic health information…."

Health IT Developers of Certified Health IT and HINs/HIEs

"…**knows, or should know**, that such practice is likely to interfere with the access, exchange or use of electronic health information…."

The regulations incorporate the knowledge standards found in the information blocking statute's definition of information blocking

(*see 45 CFR 171.103 and 42 U.S.C. 300jj-52(a)(1)(B)*)

Access, Exchange, and Use

- ***Access*** means the ability or means necessary to make electronic health information available for exchange or use.
- ***Exchange*** means the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks.
- ***Use*** means the ability for electronic health information, once accessed or exchanged, to be understood and acted upon.

> Similarly to "understood," "acted upon" within the final definition encompasses the ability to read, write, modify, manipulate, or apply the information from the proposed definition. We also clarify that "use" is bi-directional (to note, we also clarified above in the "exchange" discussion that "exchange" is bi-directional). Thus, an actor's practice could implicate the information blocking provision not only if the actor's practice interferes with the requestor's ability to read the EHI (one-way), but also if the actor's practice interferes with the requestor's ability to write the EHI (bi-directional) back to a health IT system. (85 FR 25806)

"Interfere with" or "interference" means to prevent, materially discourage, or otherwise inhibit. **(45 CFR 171.102)**

Practice Examples (illustrative purposes only) If I . . .	**Unlikely to be an Interference***	**Likely to be an Interference***	**Start to Learn More**
. . .have implemented a patient portal that includes the capability for patients to directly transmit or request direct transmission of their EHI to a third party, but I choose not to enable the capability.		✓	*Practices that May Implicate Information Blocking* in the ONC Cures Act Final Rule and *Examples of Practices Likely to Interfere* in the ONC Cures Act Proposed Rule
. . . have the capability to provide same-day access to EHI in the manner requested by a patient or a patient's health care provider but choose to take several days to respond.		✓	
. . . have implemented a FHIR API that supports patients' access to their EHI via app but refuse to allow publication of the "FHIR service base URL" (sometimes also referenced as "FHIR endpoint").		✓	

* *Actors' "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.*

"Interfere with" or "interference" means to prevent, materially discourage, or otherwise inhibit. (45 CFR 171.102)

Practice Examples (illustrative purposes only) If I . . .	Unlikely to be an Interference*	Likely to be an Interference*	Start to Learn More
. . .have a contract that includes unconscionable terms for the access, exchange, or use of EHI or licensing of an interoperability element, which could include, but not be limited to, requiring a software company that produced a patient access application to relinquish all IP rights to the actor or agreeing to indemnify the actor for acts beyond standard practice, such as gross negligence on part of the actor.		✓	(85 FR 25812)
. . . have conditioned access or use of customer EHI on revenue-sharing or royalty agreements that bear no plausible relation to the costs incurred by the EHR developer to grant access to the EHI.		✓	(85 FR 25879)
. . . am an EHR developer that prevents (such as by way of imposing exorbitant fees unrelated to the developer's costs, or by some technological means) a third-party clinical decision support (CDS) app from writing EHI to the records maintained by the EHR developer on behalf of a health care provider (despite the provider authorizing the third-party app developer's use of EHI) because the EHR developer: (1) Offers a competing CDS software to the third-party app; and (2) includes functionality (*e.g.,* APIs) in its health IT that would provide the third party with the technical capability to modify those records as desired by the health care provider.		✓	(84 FR 7519)
. . . have required third-party developers to enter into business associate agreements with all of my covered entity customers as a condition of disclosing interoperability elements to third-party developers, even if the work being done is not for the benefit of the covered entities.		✓	(84 FR 7520), HIPAA FAQ

"Interfere with" or "interference" means to prevent, materially discourage, or otherwise inhibit. (45 CFR 171.102)

Practice Examples (illustrative purposes only) If I . . .	Unlikely to be an Interference*	Likely to be an Interference*	Start to Learn More
. . . delay the access, exchange, or use of EHI to or by a third-party app designated and authorized by the patient, when there is a deployed application programming interface (API) able to support the access, exchange, or use of the EHI.		✓	(89 FR 63802)
. . . as a Certified API Developer, refuse to register and enable an application for production use within five business days of completing its verification of an API User's authenticity.		✓	(45 CFR 170.404(b)(1)(ii))
. . . refuse to register a software application that enables a patient to access their EHI, which would effectively prevent its use given that registration is a technical prerequisite for software applications to be able to connect to certified API technology. *Additional Cures Act Final Rule preamble*: Such refusals in the context of patient access unless otherwise addressed in this rule would be highly suspect and likely to implicate information blocking. We note, however, that neither app registration nor the public availability of a FHIR service base URL means that an application will be able to access any EHI. On the contrary, the application would be unable to do so unless a patient authenticates themselves via an appropriate workflow or, in the case of a health care provider, the application is appropriately configured to work within the provider's IT infrastructure.		✓	(85 FR 25813)

Exceptions: Reasonable and Necessary Activities

Promote confidence in health IT infrastructure

- Privacy and security
- Patient safety

- Promote competition and innovation
- Promote standardization and interoperability

- Usability and modernization of technology
- Greater value, more choices, reduced burden

- Greater data accessibility, including for research
- Better care and equitable health outcomes

Exceptions Policy

1. Identify certain **reasonable and necessary activities** that do not constitute information blocking

2. Address practices of **significant risk** for actors not engaging in them due to uncertainty about the information blocking regulations

3. Through appropriate conditions, **limit to protect and not extend** beyond, reasonable and necessary activities

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

Manner Exception

Overview

It will not be information blocking for an actor to limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request, provided certain conditions are met.

To satisfy this exception, an actor's practice must follow the applicable condition(s) of the exception:

Manner Requested Condition

+/or

Alternative Manner Condition

Manner Exception – Manner Requested Condition

§ 171.301(a) *Manner requested.*

(1) An actor must fulfill a request for electronic health information 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.

(2) If an actor fulfills a request for electronic health information in any manner requested:

(i) Any fees charged by the actor in relation to fulfilling the request are not required to satisfy the exception in § 171.302; and

(ii) Any license of interoperability elements granted by the actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303.

Manner Exception – Alternative Manner Condition

§ 171.301(b) ***Alternative manner.*** If an actor does not fulfill a request for electronic health information in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested, the actor must fulfill the request in an alternative manner, as follows:

(1) The actor must fulfill the request without unnecessary delay in the following order of priority, starting with paragraph (b)(1)(i) of this section and only proceeding to the next consecutive paragraph if the actor is technically unable to fulfill the request in the manner identified in a paragraph.

(i) Using technology certified to standard(s) adopted in part 170 that is specified by the requestor.

(ii) Using content and transport standards specified by the requestor and published by:

(A) The Federal Government; or

(B) A standards developing organization accredited by the American National Standards Institute.

(iii) Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor.

(2) Any fees charged by the actor in relation to fulfilling the request are required to satisfy the exception in § 171.302.

(3) Any license of interoperability elements granted by the actor in relation to fulfilling the request is required to satisfy the exception in § 171.303.

Reminder: Information Blocking Exceptions and Other Laws

- 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.”
- 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.

What Are the Consequences for Information Blocking?

"Actor"	Penalty under IB Statute (42 U.S.C. 300jj-52)
Health care providers	• Appropriate disincentives
Health information networks and Health information exchanges	• Civil monetary penalties (CMPs) up to $1 million per violation
Health IT developers of certified health IT	• Civil monetary penalties (CMPs) up to $1 million per violation • Certification action which could include a termination or ban

Effective Dates:

- CMPs Final Rule effective date: September 1, 2023.
- 2024 Final Rule Establishing Disincentives for Health Care Providers effective date: July 31, 2024

Appropriate Disincentives Final Rule

Health Care Provider Disincentives

- Medicare Promoting Interoperability Program: An eligible hospital or critical access hospital (CAH) that commits information blocking will not be a meaningful electronic health record (EHR) user during the calendar year of the EHR reporting period in which OIG refers its determination to CMS.
  - The impact on an eligible hospital will be the loss of 75 percent of the annual market basket increase; for a CAH, payment will be reduced to 100 percent of reasonable costs instead of 101 percent.

- Quality Payment Program: A MIPS eligible clinician (including a group practice) that commits information blocking will not be a meaningful EHR user during the calendar year of the performance period in which OIG refers its determination to CMS.
  - The impact on a MIPS eligible clinician required to report on the MIPS Promoting Interoperability performance category will be not earning a score in the performance category (a zero score), which is typically a quarter of the total final score.

- Medicare Shared Savings Program: A health care provider that is an Accountable Care Organization (ACO), ACO participant, or ACO provider or supplier who has committed information blocking may be ineligible to participate in the program for a period of at least one year.
  - Consequently, the health care provider may not receive revenue that they might otherwise have earned through the Shared Savings Program.
  - CMS will consider the relevant facts and circumstances before applying a disincentive under the Shared Savings Program.

Transparency Provisions

ASTP will publicly post information about actors that have been determined by OIG to have committed information blocking (after any applicable appeals), including identifying the information blocking practices, actors who committed information blocking, disincentives applied (for health care providers), and where to find any other information available about the determination from a U.S. government source. This will provide transparency into how and where information blocking is occurring.

Information Blocking and the ONC Health IT Certification Program

The 21st Century Cures Act requires that HHS establish Conditions and Maintenance of Certification requirements. These include, among others, the following:

Information blocking Condition of Certification requirement: A health IT developer must not take any action that constitutes information blocking … on or after April 5, 2021. (§ 170.401)

Assurances Condition of Certification requirement: A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking **…** or any other action that may inhibit the appropriate exchange, access, and use of electronic health information. (§ 170.402(a)(1))

Report Information Blocking Portal Page

Information Blocking Portal

WHAT IS THE STATUS OF MY REPORT?

Report Information Blocking

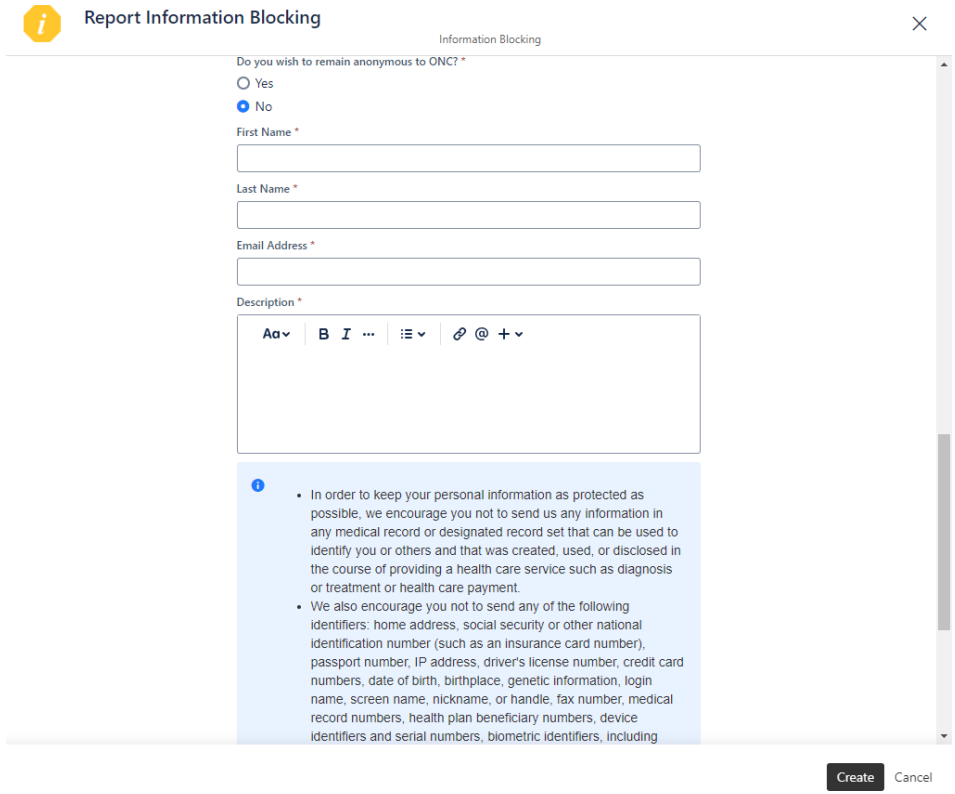
Additional Considerations:

- 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.

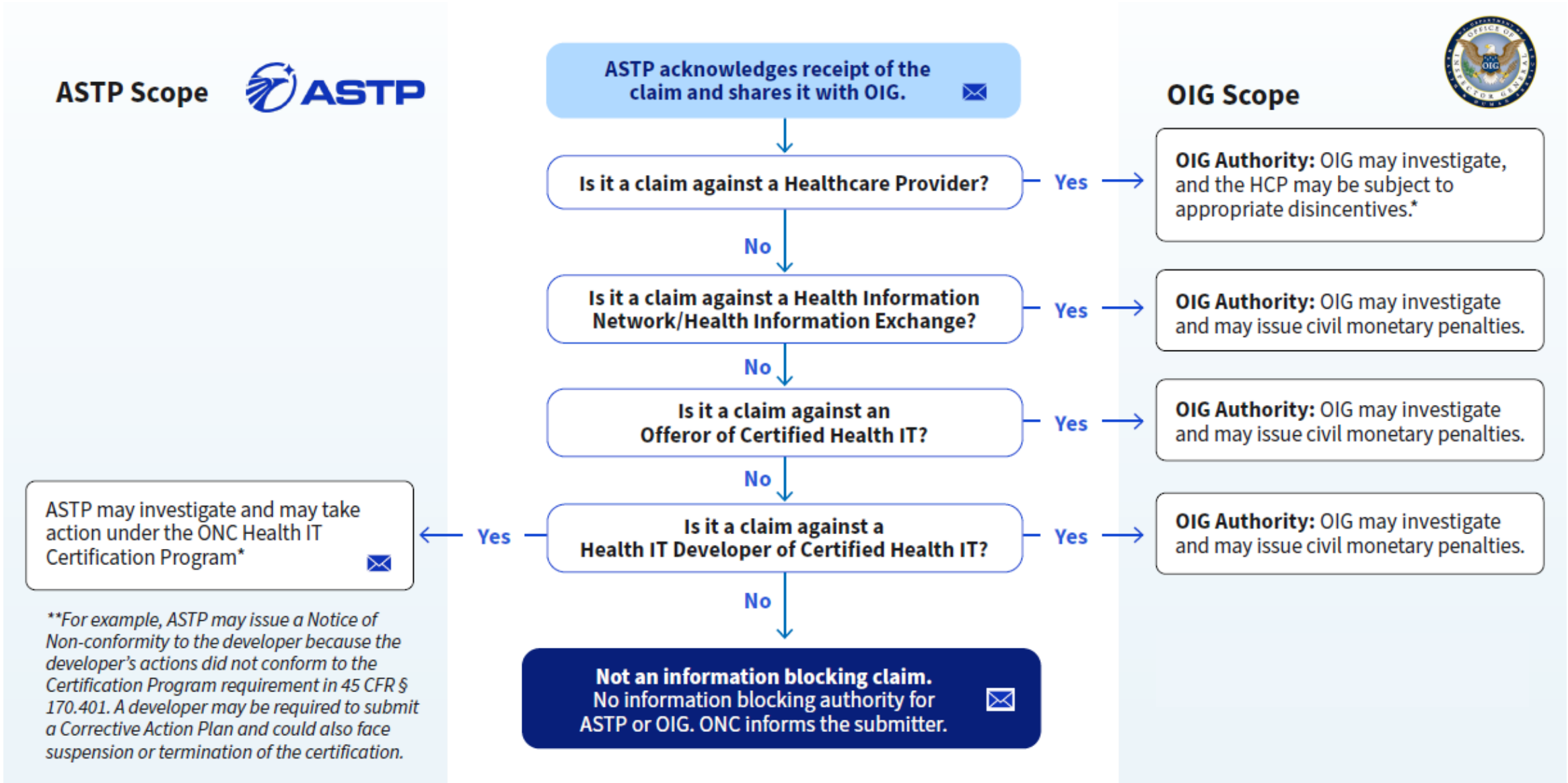
You are NOT required to submit any personally identifying information when submitting concerns, complaints, feedback, or inquires. If you want to remain anonymous to ONC, please click the "yes" button within the submission window.

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).



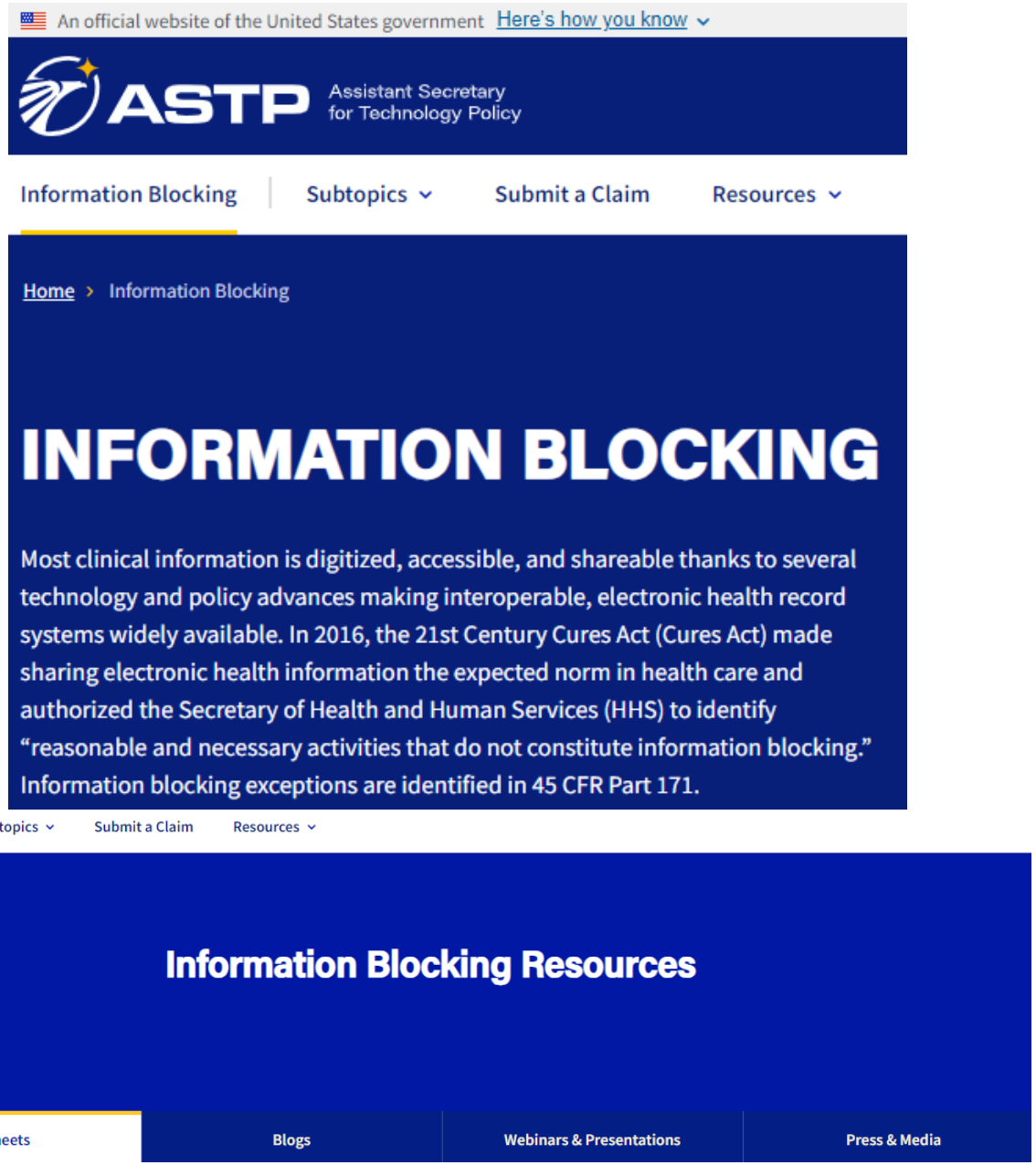
Information Blocking Portal Process – Overview



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!

Information Blocking Complaints & Enforcement Process

Scott P. Stiefel

Senior Counsel

Litigation Branch, Office of Counsel

U.S. Department of Health and Human Services, Office of Inspector General

Agenda

- Definition of Information Blocking
- OIG’s Role in Information Blocking
- Overview of Complaint & Enforcement Process

Information Blocking Definition

"Information blocking" means a practice that except as required by law or covered by an exception set forth in subpart B, C, or D of this part, is likely to interfere with access, exchange, or use of electronic health information; and

If conducted by:

A health IT developer of certified health IT, health information network or health information exchange, such developer, network or exchange knows, or should know, that the practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; or

A health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Information Blocking Definition

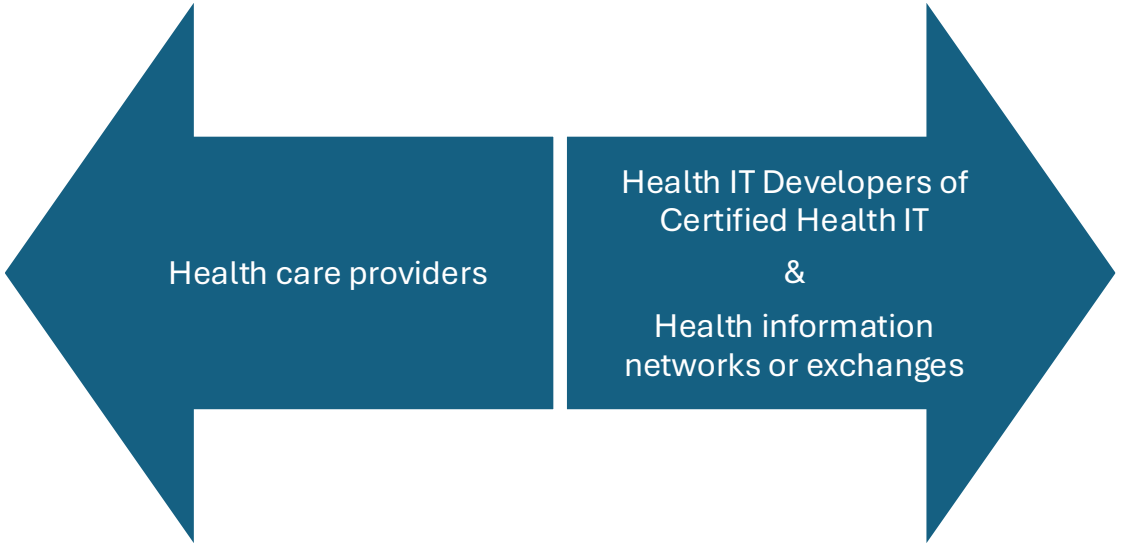
Conduct	Unless required by law or subject to an exception, a practice that is likely to interfere with the access, exchange, or use of electronic health information; and	
Actor Type	If engaged in by a health care provider,	If engaged in by a health IT developer of certified health IT, health information network, or health information exchange,
Intent	knows that such practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.	knows, or should know, the practice is likely to interfere with the access, exchange, or use of EHI.

OIG's Role in Information Blocking Enforcement

OIG may investigate any claim that:

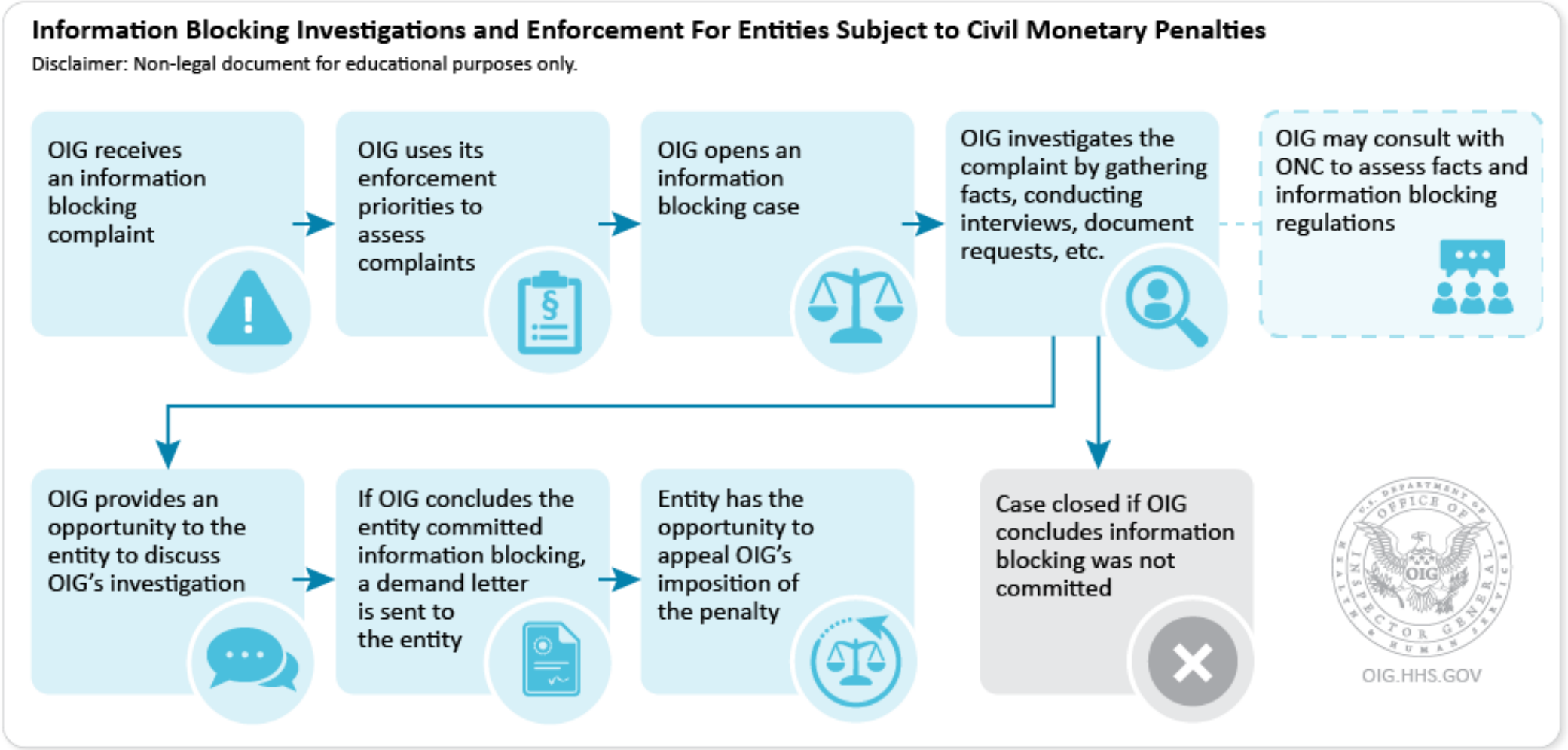
- A health IT developer of certified health IT (including an offerer of certified health IT) engaged in information blocking;
- A health information exchange or network engaged in information blocking; or
- A health care provider engaged in information blocking.

Health care provider disincentives set forth by CMS

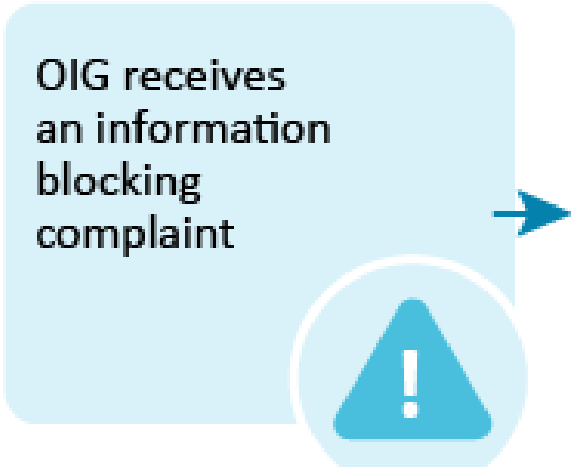


Civil Monetary Penalties (CMP)

Overview of Complaint & Enforcement Process



Information Blocking Complaints

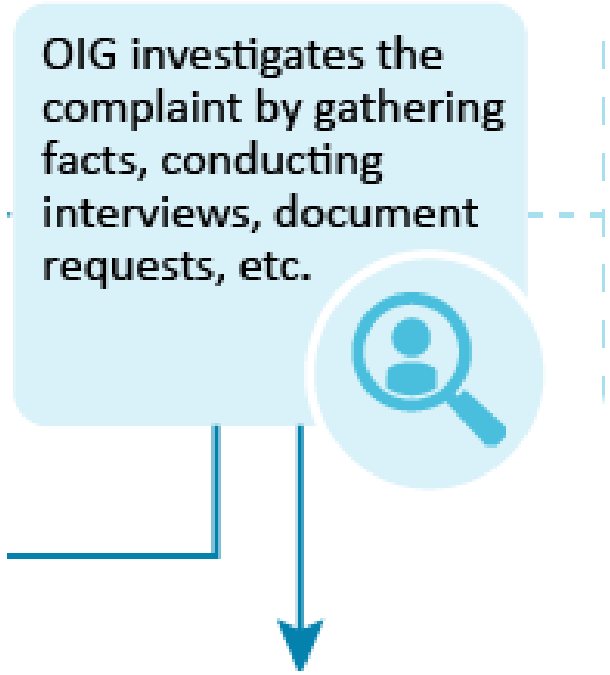


- Submission of Complaints
  - To ASTP/ONC: Information Blocking Portal
  - To OIG: OIG Hotline or 1-800-447-8477
- Potential Referrals by OIG
  - To the Assistant Secretary for Technology Policy/Office of the National Coordinator
  - To the Federal Trade Commission
  - To the Centers for Medicare & Medicaid Services
  - To the Department of Justice

OIG's Enforcement Priorities

- Enforcement priorities are:
  - (1) resulted in, is causing, or had the potential to cause patient harm;
  - (2) significantly impacted a provider's ability to care for patients;
  - (3) was of a long duration; or
  - (4) caused financial loss to Federal health care programs, or other government or private entities.
- Enforcement priorities are not dispositive
- Each allegation will be reviewed on the specific facts and circumstances

Information Blocking Investigations



- For over 35 years, OIG has conducted other CMP investigations and enforcement
- OIG will use similar methods to conduct investigations and enforcement
  - This may include:
    - Interviews
    - Document Subpoenas

Information Blocking CMP Resolutions

- Informal Notice / Monetary Settlement
- Demand Letter
- Appeal of Demand