

Information Blocking 101

Review

Michael L. Lipinski, JD
ASTP/ONC

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.

The Information Blocking Definition – § 171.103

§ 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 this part](#), 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.

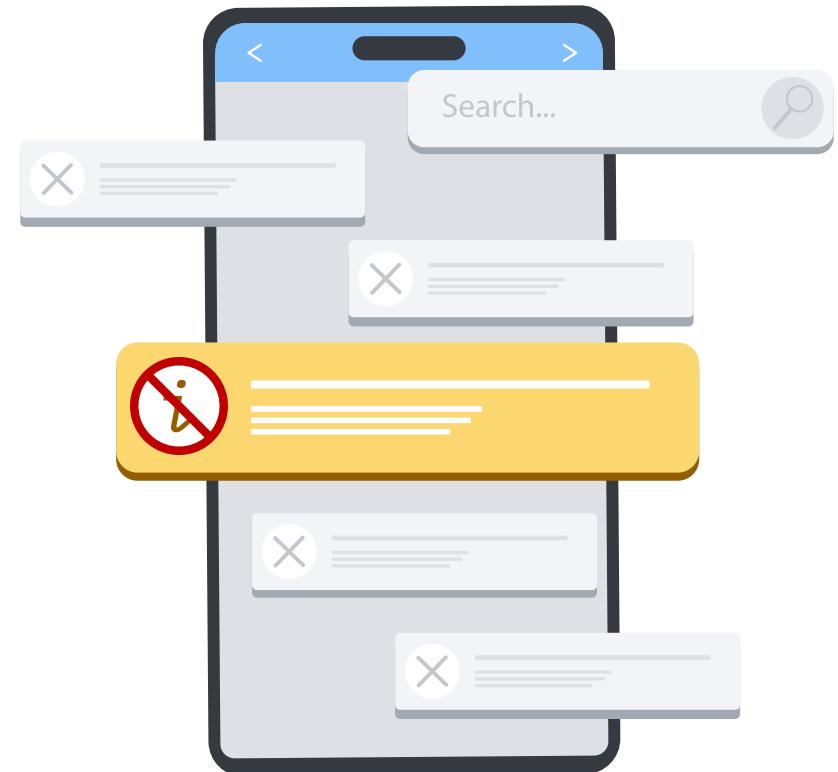
Interfere with or *interference* means to prevent, materially discourage, or otherwise inhibit.

Elements of the Information Blocking Definition

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

- Not be required by law;
- 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.





Required by Law

What does it mean?

- Refers specifically to 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.”

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

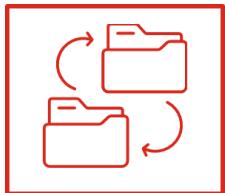
Information blocking prohibition applies to three types of “actors”



Health Care Providers



Health IT Developers of
Certified Health IT



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

Each actor is uniquely and
individually 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.

The term “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 PHSA § 3022(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](#))

Practice Examples (illustrative purposes only) If I . . .	Unlikely to be an Interference*	Likely to be an Interference*	Start to Learn More
<p>. . . 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.</p>		✓	<p><u>Practices that May Implicate Information Blocking</u> in the ONC Cures Act Final Rule</p>
<p>. . . 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.</p>		✓	<p>and</p> <p><u>Examples of Practices Likely to Interfere</u> in the ONC Cures Act Proposed Rule</p>
<p>. . . 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”).</p>		✓	

* 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.

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

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))
<p>. . . 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.</p> <p><i>Additional Cures Act Final Rule preamble:</i> 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.</p>		✓	(85 FR 25813)

Exceptions: Reasonable and Necessary Activities

Promote confidence in health IT infrastructure

- Privacy and security
- Patient safety
- Promote competition and innovation
- Usability and modernization of technology
- Greater value, more choices, reduced burden
- Promote standardization and interoperability
- Greater accessibility, including for research
- Better quality 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
-  7. Manner Exception
-  8. Fees Exception
-  9. Licensing Exception
-  10. TEFCA Manner Exception

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

What Are the Consequences for Information Blocking?

“Actor”	Penalty
Health care providers	<ul style="list-style-type: none">Appropriate disincentives
Health information networks and Health information exchanges	<ul style="list-style-type: none">Civil monetary penalties (CMPs) up to \$1 million per violation
Health IT developers of certified health IT	<ul style="list-style-type: none">Civil monetary penalties (CMPs) up to \$1 million per violationCertification 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

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)

Communications Condition and Maintenance of Certification - § 170.403

Conditions of Certification

A health IT developer may not prohibit or restrict communication of the following:

- (1) Usability
- (2) Interoperability
- (3) Security
- (4) User's experiences when using the health IT
- (5) Business practices of developers related to exchanging EHI
- (6) Manner in which a user of the health IT has used such technology

Maintenance of Certification

A health IT developer must notify all customers that any communication or contract/agreement provision that violates the Communication Condition of Certification will not be enforced.

Note: A health IT developer is required to amend contracts/agreements to remove or void such provisions when the contracts/agreements are modified for other purposes.

Communications Condition of Certification - § 170.403

Unqualified Protection For Certain Communications

- Making a disclosure required by law;
- Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;
- Communicating information about cybersecurity threats and incidents to government agencies;
- Communicating information about information blocking and other unlawful practices to government agencies; or
- Communicating information about a health IT developer's failure to comply with a Condition of Certification requirement, or with any other requirement of this part, to ONC or an ONC-ACB.

Communications Condition of Certification - § 170.403

Permitted Prohibitions and Restrictions

- Developer employees and contractors
- Non-user-facing aspects of health IT
- Intellectual property, provided that—
 - ✓ No broader than necessary to protect the developer's legitimate intellectual property interests consistent with the permitted prohibitions and restrictions.
 - ✓ It does not restrict or preclude a public display of a portion of a work subject to copyright protection (without regard to whether the copyright is registered) that would reasonably constitute a “fair use” of that work.

Communications Condition of Certification - § 170.403

Permitted Prohibitions and Restrictions (Cont.)

- Screenshots and video

A health IT developer may require persons who communicate screenshots or video to —

- ✓ Not alter the screenshots or video, except to annotate the screenshots or video or resize the screenshots or video;
- ✓ Limit the sharing of screenshots to the relevant number of screenshots needed to communicate about the health IT
- ✓ Limit the sharing of video to:
 - The relevant amount of video needed to communicate about the health IT; and
 - Only videos that address temporal matters that cannot be communicated through screenshots or other forms of communication

- Pre-market testing and development.

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>



TOPICS ▾ BLOG NEWS ▾ DATA ABOUT ASTP ▾

Home

Information Blocking

Most clinical information is digitized, accessible, and shareable thanks to several technology and policy advances making interoperable,

Information Blocking Resources

ONC publishes blogs, journal articles, and data briefs on a regular basis to ensure everyone can easily stay current with the latest findings and learnings from our work across the health IT ecosystem.

Fact Sheets

FAQs

Blogs

Webinars & Presentations

Press/Media

[Information Blocking Reminders Related to API Technology \[PDF - 271KB\]](#)

[Disincentives Common Questions \[PDF - 163KB\]](#)

[Highlighted Regulatory Dates – Information Blocking Provisions \[PDF - 330KB\]](#)

[Information Blocking Definition](#)

[Information Blocking Terms Defined](#)

[Understanding Electronic Health Information \(EHI\) \[PDF - 344KB\]](#)

[Disincentives Final Rule Overview \[PDF - 224KB\]](#)

[Health Care Provider Definition \[PDF - 446KB\]](#)

[Information Blocking Actors \[PDF - 147KB\]](#)

[Information Blocking Exceptions \[PDF - 161KB\]](#)

[Information Blocking Portal Process \[PDF - 233KB\]](#)

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](https://twitter.com/@HHS_TechPolicy)
-  [Assistant Secretary for Technology Policy](https://www.linkedin.com/in/AssistantSecretaryforTechnologyPolicy)
-  www.youtube.com/@HHS_TechPolicy

Subscribe to our weekly eblast at [healthit.gov](https://www.healthit.gov) for the latest updates!