Understanding the Information Blocking Rule: Compliance and Exceptions

1

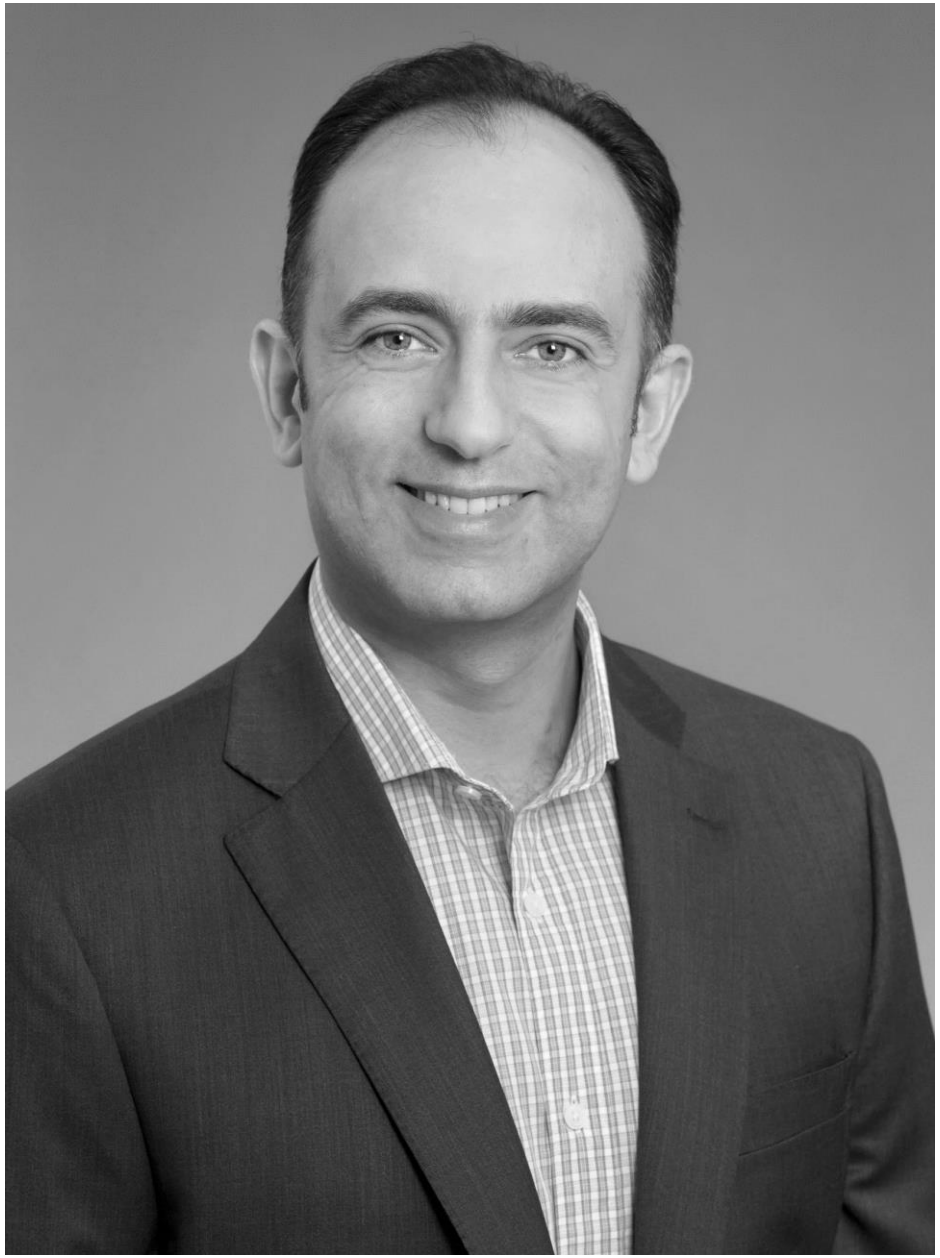
Reza Ghafoorian, MD, Esq.

G2Z Law Group, PLLC

G2Z Law Group, PLLC

Reza Ghafoorian, M.D., Esq.
Healthcare Attorney

Rghafoorian@g2zlaw.Com
(202) 656-8387



Disclaimer

EVERYTHING WE DISCUSS TODAY IS OPINION

WE ARE NOT DISPENSING LEGAL ADVICE

LISTENING DOES NOT ESTABLISH AN ATTORNEY-CLIENT RELATIONSHIP

Regulatory History

Office of the National Coordinator for Health Information Technology (ONC) published:

- Information Blocking Rule on May 1, 2020
  - Went into effect on June 30, 2020
  - Compliance deadline was November 2, 2020
- Information Blocking Interim Final Rule on November 4, 2020
  - Extended Effective date to **April 5, 2021**

What is Information Blocking?

A PRACTICE BY AN ACTOR THAT INTERFERES WITH ACCESS, EXCHANGE, OR USE OF ELECTRONIC HEALTH INFORMATION (EHI),

EXCEPT AS REQUIRED BY LAW OR SPECIFIED BY THE SECRETARY PER RULEMAKING

Requisite Legal Elements for an Information Blocking Claim

An **actor** regulated by the Information Blocking Rule

Electronic health information (EHI)

A practice that is likely to **interfere with the access, exchange, or use** of EHI

Requisite **intent** by the actor

The practice is **not required by law**

The practice is not covered by one or more of **8 regulatory exceptions**

Terminology

Engages in a practice = An act or omission

Likely to interfere with access, exchange or use = There is a reasonably foreseeable risk (even if harm does not materialize) that practice will prevent, materially discourage, or otherwise inhibit access, exchange or use of EHI

Access = The ability or means necessary to make EHI available for exchange or use

Exchange = The ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks

Use = The ability for EHI, once accessed or exchanged, to be understood and acted upon

What is Electronic Health Information (EHI)?

EHI includes Electronic Protected Health Information (ePHI) that is in a designated record set.

Designated Record Set includes:

1. Medical and Billing records of patient; and
2. Other records used by healthcare provider to make decisions about patient.

EHI does *NOT* include:

1. Psychotherapy notes;
2. Deidentified data; or
3. Information compiled in reasonable anticipation of legal proceedings.

Who are the Actors?

- Health Care Providers
- Health Information Networks or Health Information Exchange
- Health IT Developers of Certified Health IT

Requisite Intent for Actors

- Health IT Developers and Health Information Exchanges:
  - **Knows or should have known** that practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI
- Health Care Providers:
  - **Knows** that such practice is unreasonable and likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI

What Does It Mean for Clinicians and Hospitals?

- Making patient data requests easy and inexpensive
- Allowing choice of apps
- Implement
- Improving patient safety

What Does It Mean for Patients?

- Ease of access to their records
- Protecting patient privacy and security
- Promoting the ability to shop for care and manage costs

Examples of Information Blocking Acts

Internal policies more restrictive than regulations: "A health system's internal policies or procedures require staff to obtain an individual's written consent before sharing any of a patient's EHI with unaffiliated providers for treatment purposes even though obtaining an individual's consent is not required by state or federal law."

Misunderstanding the law: "A health system incorrectly claims that the HIPAA Rules or other legal requirements preclude it from exchanging EHI with unaffiliated providers."

Engineering difficult EHI flow: "A hospital directs its EHR developer to configure its technology so that users cannot easily send electronic patient referrals and associated EHI to unaffiliated providers, even when the user knows the Direct address and/or identity (i.e., National Provider Identifier) of the unaffiliated provider."

Examples of Information Blocking Acts

Unnecessary delays: “A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient’s health care provider, but takes several days to respond.”

Requiring to adopt non-interoperable EHR: “A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians that do not comply.”

Discrimination against EHI vendors: “A health care provider imposes one set of fees and terms to establish interfaces or data sharing arrangements with several registries and exchanges, but offers another more costly or significantly onerous set of terms to establish substantially similar interfaces and arrangements with an HIE or HIN that is used primarily by health plans that purchase health care services from the provider at negotiated reduced rates.”

Practices that are NOT Information Blocking

Interference with use, exchange and access to EHI when:

- Required by Law
  - e.g., statutes, regulations, court order, binding administrative decisions, settlements, tribal law, etc.
- Covered by eight (8) exceptions
- Done by the actor without the required level of intent

Eight Exceptions


Category of Exceptions

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

- *Preventing Harm*
- *Privacy*
- *Security*
- *Infusibility*
- *Health IT Performance*

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

- *Licensing*
- *Fees*
- *Content and Manner*

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

Preventing Harm Exception

It will not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.

This exception recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI.

Key Conditions of the Exception

- The actor must hold a reasonable belief that the practice will substantially reduce a risk of harm to a natural person;
- The actor's practice must be no broader than necessary;
- The actor's practice must satisfy at least one condition from each of the following categories: type of risk, type of harm, and implementation basis; and
- The practice must satisfy the condition concerning a patient right to request review of an individualized determination of risk of harm.

Privacy Exception

It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy, provided certain conditions are met.

This exception recognizes that if an actor is permitted to provide access, exchange, or use of EHI under a privacy law, then the actor should provide that access, exchange, or use. However, an actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws.

Key Conditions of the Exception

To satisfy this exception, an actor's privacy-protective practice must meet at least one of the four sub-exceptions:

1. ***Precondition not satisfied:*** If an actor is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use of EHI, the actor may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances.
2. ***Health IT developer of certified health IT not covered by HIPAA:*** If an actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, the actor may choose to interfere with the access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are met.
3. ***Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a) (1) and (2):*** An actor that is a covered entity or business associate may deny an individual's request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.
4. ***Respecting an individual's request not to share information:*** An actor may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided certain conditions are met.

Security Exception

It will not be information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.

This exception is intended to cover all legitimate security practices by actors, but does not prescribe a maximum level of security or dictate a one-size-fits-all approach.

Key Conditions of the Exception

- The practice must be:
  - Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
  - Tailored to specific security risks; and
  - Implemented in a consistent and non-discriminatory manner.
- The practice must either implement a qualifying organizational security policy or implement a qualifying security determination.

Infeasibility Exception

It will not be information blocking if an actor does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided certain conditions are met.

This exception recognizes that legitimate practical challenges may limit an actor's ability to comply with requests for access, exchange, or use of EHI. An actor may not have—and may be unable to obtain—the requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use.

Key Conditions of the Exception

- The practice must meet one of the following conditions:
  - Uncontrollable events: The actor cannot fulfill the request for access, exchange, or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
  - Segmentation: The actor cannot fulfill the request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI.
  - Infeasibility under the circumstances: The actor demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.
- The actor must provide a written response to the requestor within **10 business days** of receipt of the request with the reason(s) why the request is infeasible.

Health IT Performance Exception

It will not be information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.

This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that health IT be taken offline temporarily. Actors should not be deterred from taking reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of health IT.

Key Conditions of the Exception

- The practice must:
    1. Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
    2. Be implemented in a consistent and non-discriminatory manner; and
    3. Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN.
- An actor may take action against a third-party app that is negatively impacting the health IT's performance, provided that the practice is:
    1. For a period of time no longer than necessary to resolve any negative impacts;
    2. Implemented in a consistent and non-discriminatory manner; and
    3. Consistent with existing service level agreements, where applicable.
- If the unavailability is in response to a risk of harm or security risk, the actor must only comply with the Preventing Harm or Security Exception, as applicable.

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

Licensing Exception

It will not be information blocking for an actor to license interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.

This exception allows actors to protect the value of their innovations and charge reasonable royalties in order to earn returns on the investments they have made to develop, maintain, and update those innovations.

Key Conditions of the Exception

The practice must meet:

- The negotiating a license conditions: An actor must begin license negotiations with the requestor within 10 business days from receipt of the request and negotiate a license within 30 business days from receipt of the request.
- The licensing conditions:
  - Scope of rights
  - Reasonable royalty
  - Non-discriminatory terms
  - Collateral terms
  - Non-disclosure agreement
- Additional conditions relating to the provision of interoperability elements.

Fees Exception

It will not be information blocking for an actor to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.

This exception enables actors to charge fees related to the development of technologies and provision of services that enhance interoperability, while not protecting rent seeking, opportunistic fees, and exclusionary practices that interfere with access, exchange, or use of EHI.

Key Conditions of the Exception

The practice must:

- Meet the basis for fees condition.
  - For instance, the fees an actor charges must:
    - Be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests.
    - Be reasonably related to the actor's costs of providing the type of access, exchange, or use of EHI.
    - Not be based on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor.
- Not be specifically excluded.
  - For instance, the exception does not apply to:
    - A fee based in any part on the electronic access by an individual, their personal representative, or another person or entity designated by the individual to access the individual's EHI.
    - A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10).
- Comply with Conditions of Certification in § 170.402(a)(4) (Assurances – certification to "EHI Export" criterion) or § 170.404 (API).

Content and Manner Exception

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 to access, exchange, or use EHI, provided certain conditions are met.

This exception provides clarity and flexibility to actors concerning the required content (i.e., scope of EHI) of an actor's response to a request to access, exchange, or use EHI and the manner in which the actor may fulfill the request. This exception supports innovation and competition by allowing actors to first attempt to reach and maintain market negotiated terms for the access, exchange, and, use of EHI.

Key Conditions of the Exception

- ***Content Condition:*** Establishes the content an actor must provide in response to a request to access, exchange, or use EHI in order to satisfy the exception.
    1. Up to 24 months after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard.
    2. On and after 24 months after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange, or use EHI with EHI as defined in § 171.102.
- ***Manner Condition:*** Establishes the manner in which an actor must fulfill a request to access, exchange, or use EHI in order to satisfy this exception.
    - An actor may need to fulfill a request in an ***alternative manner*** when the actor is:
        - Technically unable to fulfill the request in any manner requested; ***or***
        - Cannot reach agreeable terms with the requestor to fulfill the request.
    - If an actor fulfills a request in an alternative manner, such fulfillment must comply with the order of priority described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

Enforcement & Penalties

Enforcement body:

- OIG enforces the Information Blocking Rule.

Penalties:

- Civil Monitory Penalty (CMP) of up to $1 million per violation if actor is a Health IT Developer of Certified Health Information Technology (CHIT) or Health Information Network (HIN)/Health Information Exchange (HIE)
- OIG will refer healthcare providers to appropriate agency (e.g., CMS or OCR) to be subjected to appropriate disincentives.

How to get ready to comply?

1. Start an information blocking compliance workgroup. That is, identify an organizational leader and create a multi-disciplinary information blocking compliance team (*e.g.*, legal, clinical, IT) to identify, assess, implement and advocate for organizational compliance.
2. Review, update and, if necessary, create organizational policies, procedures and processes for compliance.
3. Train workforce members on information blocking compliance, including assessment of workforce member knowledge following the training. Training should be ongoing and not be a one-time event. Health care providers should consider combining their information blocking training with their HIPAA compliance training.
4. Implement a complaint process for identification and reporting of information blocking complaints (including anonymous reporting).
5. Monitor, investigate and enforce compliance through regular risk assessments and complaint investigations. Remediate any issues, including implementing corrective action plans and disciplining workforce members, as appropriate.
6. Identify and assess any vendors that exchange, use or access EHI and request confirmation of the vendor's own compliance program and confirmation that the vendor does not engage in information blocking.
7. Review and amend, as necessary, contracts and agreements that impose restrictions on the other party's access, exchange or use of EHI for compliance with the regulatory safe harbors.

Resources

- ONC Information Blocking Rule
- The Sequoia Project
- AMA – What is information blocking?
- AMA – How to comply with info blocking and where do I start?

G2Z Law Group, PLLC

Reza Ghafoorian, M.D., Esq.

Principal Attorney

info@g2zlaw.Com

(202) 656-8387