This is a copy of the May 12, 2021, AIHC Blog Article

HIPAA, The Cures Act and Information Blocking Compliance

The patient is at the center of the 21st Century Cures Act. Putting patients in charge of their health records is a key piece of patient control in health care, and patient control is at the center of HHS' work toward a value-based health care system. Patients need more power in their health care, and access to information is key to making that happen.

The Office of the National Coordinator for Health Information Technology (ONC) Cures Act Final Rule implements interoperability requirements outlined in the Cures Act.

HIPAA security requires covered entities to protect health information. This information blocking practice is allowed except as required by law or as specified by the Secretary of Health and Humans Services as a reasonable and necessary activity. However, it is likely to interfere with access, exchange and/or use of electronic health information (EHI).

- EHI is defined as the electronic protected health information (ePHI) in a designated record set (as defined in the Health Insurance Portability and Accountability Act (HIPAA) regulations) regardless of whether the records are used or maintained by or for a covered entity. The designated record set in a physician's practice typically includes:

    - Medical records and billing records about individuals;
    - Other records used, in whole or in part, by physicians to make decisions about individuals

Why is this important to you?

All Actors will be subject to ONC's Information Blocking rules and regulations on **April 5, 2021**.

For the first 24 months after publication of the Final Rule (***currently until August 2, 2022***), for the purposes of the information blocking definition, EHI is limited to the data elements represented in the US Core Data for Interoperability (USCDI) V1 standard adopted in the Final Rule.

- EHR vendors are currently updating their products to support the access, exchange, and use of all data elements in the USCDI. This will take time and, for some smaller EHR vendors, may take several months.

- After August 2, 2022, the definition of EHI expands to that of ePHI described above. At that time, all physicians will be required to make their patients' ePHI available for access, exchange, and use.

Penalties - Because there are investigations, penalties and disincentives! Actors that are subject to the information blocking regulations may be investigated by the HHS Office of Inspector General (OIG) if they are the subject of a claim of information blocking.

Further, actors found to have committed information blocking are subject to penalties:

- Health IT developers of certified health IT, health information networks, and health information exchanges → Civil monetary penalties (CMPs) up to $1 million per violation

- Health care providers → Appropriate disincentives to be established by the Secretary

Got Your Attention?

What is behind the Information Blocking and Need to Comply?

The 21st Century Cures Act (Cures) is a landmark bipartisan health care innovation law enacted in December 2016. Cures includes provisions to promote health information interoperability and prohibit information blocking or "info blocking" by "Actors." Actors are considered:

- Health Care Providers;
- Health Information Networks (HIN) and Health Information Exchanges (HIE); and
- Health information technology (IT) developers.

In March 2019, the Office of the National Coordinator for Health Information Technology (ONC) issued a Proposed Rule, 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program. They released a final rule in March 2020 and published it in the Federal Register on May 1, 2020.

What are examples of practices that could constitute information blocking?

Section 4004 of the Cures Act specifies certain practices that could constitute information blocking:

- Practices that restrict authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies (health IT);

- Implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI;

- Implementing health IT in ways that are likely to—
    - Restrict the access, exchange, or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems; or
    - 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.

Additional examples of practices that could constitute information blocking can be found on the Office of the National Coordinator for Health Information Technology (ONC) website at: https://www.healthit.gov/curesrule/

Ah – there are Exceptions!

What are the information blocking exceptions?

Section 4004 of the Cures Act authorizes the Secretary of HHS to identify reasonable and necessary activities that do not constitute information blocking. The exceptions support seamless and secure access, exchange, and use of EHI and offer actors certainty that practices that meet the conditions of an exception will not be considered information blocking.

A practice that does not meet the conditions of an exception would not automatically constitute information blocking. Such practices would not have guaranteed protection from civil monetary penalties or appropriate disincentives and would be evaluated on a case-by-case basis to determine whether information blocking has occurred. Physicians must satisfy ALL applicable conditions of an exception at all relevant times to meet the exception as it relates to the access, exchange, and use of EHI. Each exception is limited to certain practices that clearly advance the aims of ONC's Final Rule and are tailored to align with the following criteria:

- ***Be reasonable and necessary***
  These reasonable and necessary practices include providing appropriate protections to prevent harm to patients and others; promoting the privacy and security of EHI; promoting competition and innovation in health IT and its use to provide health care services to consumers, and to develop an efficient means of health care delivery; and allowing system downtime to implement upgrades, repairs, and other changes to health IT.

- ***Address significant risk***
  The exceptions are intended to address what ONC considers a "significant risk" and that Actors would otherwise avoid engaging in out of concern that such activities could be interpreted as info blocking.

- ***Subject to strict conditions***
  Each exception is subject to strict conditions to ensure practices are limited to those that are reasonable and necessary.

Exceptions are divided into two classes in the Cures Act Final Rule:

- Exceptions that involve not fulfilling requests to access, exchange, or use EHI; and
- Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

In the final rule, they have identified ***eight categories*** of reasonable and necessary activities that do not constitute information blocking, provided certain conditions are met (referred to as "exceptions"). The information below is a summary. Go to healthIT.gov for more information.

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

1. **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.

Physicians must hold a reasonable belief that the practice will substantially reduce the risk of physical harm to a patient or another natural person and the practice is no broader than necessary to substantially reduce the risk of harm. Practices include:

- Declining to share data that is corrupt, inaccurate, or erroneous.
- Declining to share data arising from misidentifying a patient or mismatching a patient's EHI.
- Refraining from a disclosure that would endanger life or physical safety of a patient or another person.
    - The licensed provider who made the determination must have done so in the context of a current or prior clinician-patient relationship.

Patients may opt to appeal a physician's use of the Harm Exception. Physicians must implement their practice in a way that allows for the patient whose EHI is affected to exercise their rights under HIPAA or any federal, state, or tribal law to have the determination reviewed and potentially reversed.

The practice must be consistent with a written organizational policy that is:

- Based on relevant clinical, technical, other appropriate expertise;
- Implemented in a consistent and non-discriminatory manner; and
- Conforms each practice to the conditions in the harm exception.

2. 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.

Sub-exceptions

- *Unsatisfied legal precondition to the release of EHI*

    a. Physicians may withhold EHI if a state or federal privacy law imposes preconditions for providing access, exchange or use of EHI (e.g., a requirement to obtain a patient's consent before disclosing the EHI), if their practice:

        i. Is tailored to the applicable precondition;
        ii. Implemented in consistent and non-discriminatory manner; and
        iii. Either:
            - Conforms to physician's written organizational policies; or
            - Is documented by a physician on a case-by-case basis

- *Certified health IT developer not covered by HIPAA*

- *Denial of individual's request for ePHI consistent with the HIPAA Privacy Rule*

    a. HIPAA covered entity or business associate Actor may deny an individual's request for EHI under the HIPAA Privacy Rule's right of access if the Actor's practice complies with the Privacy Rule's "unreviewable grounds" for a denial of access.

        i. Unreviewable grounds under Privacy Rule:
            - Certain requests made by inmates of correctional institutions;
            - Information created or obtained during research that includes treatment if certain conditions are met;
            - Denials permitted by the federal Privacy Act; and
            - Information obtained from non-health care providers pursuant to promises of confidentiality.

Respecting an individual's request not to share information

a. An Actor may decline to provide access, exchange, or use of EHI if it meets the following requirements intended to align with an individual's HIPAA Privacy Rule right to request additional restriction:

    i. Individual requests that the Actor not provide such access, exchange, or use of the EHI without any improper encouragement or inducement of the request by the Actor.

3. 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.

General conditions — A practice is not info blocking if it is:

- Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
- Tailored to the specific security risk being addressed; and
- Implemented in a consistent and non-discriminatory manner.

Actors and their security-related practices may satisfy proposed exception through:

- Written organizational policies; or
- Determinations on a case-by-case basis under particular facts and circumstances.

A practice must meet both:

- General conditions; and
- Either the requirements for organizational policies or case-by-case determinations.

For practices that do not implement an organizational security policy, an Actor must have decided in each case, based on the particular facts and circumstances, that:

- The practice is necessary to mitigate the security risk to EHI; and
- There are no reasonable alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

4. 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. To receive protection, the practice must meet one of the following conditions:

- Uncontrollable Events: The Actor cannot fulfil the request for access, exchange, or use of EHI 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 fulfil the request for access, exchange, or use of EHI because the Actor cannot unambiguously segment the requested EHI from EHI that:

  - Cannot be made available due to a patient's preference or because the EHI cannot be made available by law; or

  - May be withheld in accordance with the Preventing Harm Exception.

- Infeasible Under the Circumstances: The Actor demonstrates, prior to responding to the request, 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.

* *You may need to provide access to information that is not otherwise protected by federal or state privacy law (e.g., HIPAA Patient Right of Access). You should consider speaking with your compliance officer or practice manager about how to handle such situations. For example, you may still be required to print out an office note and hand redact protected information even if you claim the Infeasibility Exception.*

5. 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. An Actor's practice to maintain or improve health IT performance is not info blocking when the practice meets one of the four following conditions:

- Maintenance and improvement to health IT (e.g., an EHR upgrade).
- Consistent with existing service level agreements, where applicable.
- Practices that prevent harm and comply with Preventing Harm Exception.
- Security-related practices that comply with Security Exception.

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

6. Content and Manner Exception

This is an important exception for physicians who are limited by their EHR vendor's ability to access, use, or exchange patient information. Physicians are encouraged to discuss the use of this exception with their EHR vendor. If the burden on the Actor for fulfilling a request is so significant that the Actor chooses to not fulfil the request at all, the Actor could seek coverage under the Infeasibility 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. This exception applies to practices that involve the Actor responding to a request with limited information and in a manner other than what was requested by the requestor.

- Content:
  - For 24 months after final rule publication, the Actor must respond with the subset of EHI identified by the USCDI data elements.
  - After that date, the Actor must respond with all EHI in a designated record set (i.e., ePHI).

- Manner of Response: The Actor must respond either:
  - In the manner requested; or
  - In an alternative manner.

7. 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.

Fees may result in a reasonable profit. The exception excludes certain fees, such as those based on electronic access to EHI by the individual. ONC divided the Fee Exception into three conditions.

- To qualify for this exception, the Actor's practice must meet the "Basis of fees condition," not include any of the fees addressed in the "Excluded fees condition," and comply with the "Compliance with the Conditions of Certification condition" if the Actor is a health IT developer subject to ONC's Conditions of Certification (CoC).
- This exception will most likely be applicable to EHR vendors rather than physicians or other providers.

8. 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.

Conclusion

Information blocking can occur in many forms for both Actors and Patients. Physicians can experience information blocking when trying to access patient records from other providers, connecting their EHR systems to local health information exchanges, migrating from one EHR to another, and linking their EHRs with a clinical data registry. Patients can also experience information blocking when trying to access their medical records or when sending their records to another provider.

The new rules regulate EHR vendors, prohibiting them from blocking information. Like physicians, EHR vendors must comply with these regulations ***now***. Learn more by reviewing the resources provided below.

Resources

American Medical Association –

- ***How Do I Comply With Info Blocking and Where Do I Start?***
  https://www.ama-assn.org/system/files/2020-11/info-blocking-compliance.pdf

- ***How doctors can adjust to new reality—opening notes to patients*** (Posted March 2, 2021)
  https://www.ama-assn.org/practice-management/digital/how-doctors-can-adjust-new-reality-opening-notes-patients

ONC

- ***Fact Sheets***
  https://www.healthit.gov/curesrule/resources/fact-sheets

- ***Cures Act Final Rule***
  https://www.healthit.gov/curesrule/download

- ***Differences Between the Proposed and Final Rule***
  https://www.healthit.gov/curesrule/overview/major-changes-proposed-rule-final-rule

- ***HealthITBuzz: A New Day for Interoperability – The Information Blocking Regulations Start Now*** (Posted April 5, 2021)
  https://www.healthit.gov/buzz-blog/information-blocking/a-new-day-for-interoperability-the-information-blocking-regulations-start-now