AMA
AMERICAN MEDICAL ASSOCIATION

PART 1

What is information blocking?

Information blocking (info blocking) can occur in many forms. Physicians can experience info blocking when trying to access patient records from other providers, connecting their electronic health record (EHR) systems to local health information exchanges (HIEs), migrating from one EHR to another, and linking their EHRs with a clinical data registry. Patients can also experience info blocking when trying to access their medical records or when sending their records to another provider. AMA policy supports legislative and regulatory prohibitions on info blocking and is a longstanding advocate of eliminating major contributors to info blocking by EHR vendors. These include:

- Restrictive and unfair contractual limitations on physicians' use and exchange of medical information;
- Excessive fees charged to create EHR interfaces or connections with other health information technology (health IT); and
- Technical or non-standard methods of implementing EHRs and other health IT that block the access, exchange, or use of medical information.

Reflecting longstanding concerns raised by the AMA, patients, and health care community stakeholders, 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 info blocking by "Actors," which are health information networks, HIEs, health information technology developers of certified health IT, and health care providers.

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* and released a final rule in March 2020, published in the Federal Register on May 1, 2020.

Key terms in the information blocking rules and regulations

Cures defines info blocking as business, technical, and organizational practices that prevent or materially discourage the access, exchange or use of **electronic health information** (EHI) when an ***Actor knows***, or (for some Actors like EHR vendors) **should know**, that these practices are ***likely*** to interfere with ***access, exchange, or use*** of **EHI**. If conducted by a health care provider, there must also be **knowledge that such practice is *unreasonable*** and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

The info blocking Final Rule defines "access," "exchange," and "use" as follows:

- **"Access"** is the ability or means necessary to make EHI available for exchange, use, or both.
- **"Exchange"** is the ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks; and is inclusive of all forms of transmission such as bidirectional and network-based transmission.
- **"Use"** is the ability for EHI to be understood and acted upon once accessed or exchanged. "Acted upon" includes the ability to read and write and is also bidirectional.

What is electronic health information (EHI)?

The term EHI was established by Congress in Cures; however, it was not defined in statute. Rather, ONC has defined it in their Final Rule.

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.

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.**

Who must comply and by when?

The Cures Act specified four types of entities referred to as "Actors" who must comply with info blocking requirements:

- Health care providers[1] ;
- Health IT developers of certified health IT; and
- Health Information Networks (HINs) or HIEs (HIN and HIE are combined into one defined type in the Final Rule).

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

1 Same meaning as "health care provider" at 42 U.S.C. 300jj—includes 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 IHS or by an Indian tribe, tribal organization, or urban Indian organization, rural health clinic, a covered entity ambulatory surgical center, therapist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary.

What practices are considered information blocking?

Info blocking practices can be an Actor's acts or omissions—essentially anything that interferes with the access, exchange, or use of EHI. However, just because an action interferes with the access, exchange, or use of EHI does not mean the practice is automatically considered an info blocking violation—facts and circumstances unique to each action should be taken into account. For instance, physician Actors must have the required ***knowledge and intent*** to interfere with access, exchange, or use of EHI. Info blocking practices may include but are not limited to:

1. 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;
2. Implementing health IT **in nonstandard** ways that are likely to substantially increase the **complexity or burden** of accessing, exchanging, or using EHI;
3. Limiting or restricting the interoperability of health IT, such as **disabling or restricting** the use of a capability that enables sharing EHI with users of other systems or restricting access to EHI by certain types of persons or purposes that are legally permissible, or **refusing to register a software application that enables patient access to their EHI** (assuming there is not a legitimate security reason that meets the conditions of the Security Exception, discussed further below);
4. 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**. This would include acts that make **transitions between certified health information technologies more challenging (e.g., an EHR vendor charging excessive fees or using tactics to delay a practice's switch from their EHR to another vendor's EHR);**
5. Acts that lead to **fraud, waste, or abuse**, or **impede innovations** and **advancements** in health information access, exchange, and use, including care delivery enabled by health IT;
6. Restrictions on access, exchange, and use, such as may be expressed in **contracts, license terms, EHI sharing policies, organizational policies or procedures** or other instruments or documents that set forth requirements related to EHI or health IT, such as Business Associate Agreements (BAAs); and
7. Rent-seeking (e.g., gaining larger profits by manipulating economic conditions) or other opportunistic pricing practices.

Physicians may implicate the info blocking rule if they knowingly take actions that interfere with exchange, access, and use of EHI, even if no harm materializes. A physician organization, for instance, may have a policy that restricts access to patient lab results for a certain amount of time. Even if patients are not aware there is a delay between when the results are available to the physician and when they are made available to the patient, a practice that is merely "likely" to interfere with the access, use, or exchange of EHI could be considered info blocking.

Note that physicians are not held to the same "should know" standard as in the case with EHR vendors. Physicians must know their actions would likely interfere, prevent, or materially discourage access, exchange, and use of EHI to be considered information blocking. High-risk info blocking actions include interfering with:

- Patients who seek to access their own EHI;
- Providers who seek EHI for treatment or quality improvement;
- Payers who seek EHI to confirm a clinical value; or
- Patient safety and public health.

Examples of potential violations include:

- Formal restrictions: Provider or office policy requires staff to obtain a patient's written consent before sharing any EHI with unaffiliated providers for treatment purposes.
- Technical limitations: A physician disables the use of an EHR capability that would enable staff to share EHI with users at other systems.
- Isolated interferences: A physician has the capability to provide same-day EHI access in a format requested by an unaffiliated provider—**or by their patient**—but takes several days to respond.

In its Final Rule and as required by Cures, ONC identified "reasonable and necessary" activities that are not info blocking (i.e., info blocking exceptions). ONC interprets the info blocking prohibition broadly, relying on the exceptions to carve out protected conduct. **For nearly all EHI requests, physicians must respond and release patients' medical records unless an appropriate exception can be identified and used.**

ONC's Final Rule does not trump or override other state or federal law. For instance, some state laws impose specific preconditions that must be satisfied before information can be released—such as adolescent reproductive health or HIV status information. If the specific precondition being relied upon is patient consent, and patient consent has not or cannot be obtained, then physicians should restrict access, exchange, or use of that information until the patient's consent is obtained. **Physicians are still required to follow state or federal laws applicable to the release of medical records; complying with state or federal law would likely not constitute information blocking.**

What are Exceptions?

ONC uses the term "exception" to implement a concept of reasonable and necessary activities used in Cures. Congress directed ONC to identify activities that were valid reasons to restrict information access and that would likely be considered EHI info blocking. For instance, medical practices may need to restrict access to patient records in their EHR due to data privacy or security reasons—such as when a patient's consent is required but not documented or instances of cybersecurity threats. Individuals or other entities may also request medical records from a physician's office in a manner not supported by their EHR—such as requesting documents over application programing interfaces (APIs) when APIs are not supported. There are two categories of info blocking exceptions:

1. Not fulfilling requests to access, exchange, or use EHI
    - o Preventing harm exception
    - o Privacy exception
    - o Security exception
    - o Infeasibility exception
    - o Health IT performance exception
2. Procedures for fulfilling requests to access, exchange, or use EHI
    - o Content and manner exception
    - o Fees exception
    - o Licensing exception

It is important to note that, unlike HIPAA where regulation outlines when information is **permitted** to be exchanged, info blocking regulations are **directive and require** Actors to provide access, exchange, and use of EHI for nearly all requests. **Exceptions are an important tool for physicians to use in defense of a claim that their practice is info blocking**. There are many documentation requirements embedded within exception

conditions. A major component of a physician's compliance with info blocking, and use of exceptions, is documentation. The specific facts and circumstances associated with your decision to use an exception will be important to include in your documentation.

Moreover, failing to meet the conditions of an exception does not automatically mean a practice is info blocking, only that there is not guaranteed protection from penalties or disincentives. Each act must then be evaluated on a case-by-case basis (e.g., level of impact, intent, or knowledge).

Exceptions to the definition of information blocking

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.

The following is a summary of each exception. Additional information on the exceptions can be found on ONC's website.

Preventing Harm Exception — When will an Actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to prevent harm not be considered information blocking?

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. *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.*

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.
    - o The licensed provider who made the determination must have done so in the context of a current or prior clinician-patient relationship.

Note that 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

1. Based on relevant clinical, technical, other appropriate expertise;

2. Implemented in a consistent and non-discriminatory manner; and
3. Conforms each practice to the conditions in the harm exception discussed above.

Privacy Exception — When will an Actor's practice of not fulfilling a request to access, exchange, or use EHI in order to protect an individual's privacy not be considered information blocking?

This exception recognizes that an Actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws. *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.*

The Privacy Exception consists of four "sub-exceptions." The sub-exceptions ensure individual privacy rights are not diminished as a consequence of the info blocking provision and to ensure the info blocking provision does not require the use or disclosure of EHI in a way not permitted under the HIPAA Privacy Rule.

Note that whereas the HIPAA Privacy Rule permits, but does not require, covered entities to disclose ePHI in most circumstances, **the info blocking rule requires the Actor to provide access, exchange, or use of EHI unless prohibited by law or covered by one of the exceptions.**

Sub-exceptions

1. 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:
            1. Conforms to physician's written organizational policies; or
            2. Is documented by a physician on a case-by-case basis
2. Certified health IT developer not covered by HIPAA
3. 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:
            1. Certain requests made by inmates of correctional institutions;
            2. Information created or obtained during research that includes treatment if certain conditions are met;
            3. Denials permitted by the federal Privacy Act; and
            4. Information obtained from non-health care providers pursuant to promises of confidentiality.
4. 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.

- Security Exception — When will an Actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to protect the security of EHI not be considered information blocking?

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. *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.*

The Security Exception allows Actors to implement reasonable and necessary security practices and prohibits security practices that are disguised info blocking.

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.

Infeasibility Exception — When will an Actor's practice of not fulfilling a request to access, exchange, or use EHI due to the infeasibility of the request not be considered information blocking?

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. *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.*

The Infeasibility Exception applies when it would be infeasible for an Actor to respond to a request for access, exchange, or use of EHI. In some cases, the Actor may not have or may be unable to obtain the requisite technological capabilities, legal rights, financial resources, or other means necessary to provide a particular form of access, exchange, or use. In other cases, the Actor may be able to comply with the request but only by incurring cost or other burdens that are clearly unreasonable under the circumstances.

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

- Uncontrollable Events: The Actor cannot fulfill 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 fulfill the request for access, exchange, or use of EHI because the Actor cannot unambiguously segment the requested EHI from EHI that:
    - o Cannot be made available due to a patient's preference or because the EHI cannot be made available by law; or
    - o 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.

* NOTE: 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.

Health IT Performance Exception — When will an actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of EHI not be considered information blocking?

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. The Actor's practices must be related to the maintenance and improvement of health IT (e.g., temporary unavailability of data or degradation of the performance of health IT). Actors should also be allowed to protect the resiliency of their computer network if third-party applications negatively impact the performance of their systems. These practices must last no longer than necessary. *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.*

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

Content and Manner Exception — When will an actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI not be considered information blocking?

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. Under this new exception, an Actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI will not be considered information blocking if the practice meets both a "content condition" and "manner condition." Under the content condition, **an Actor may respond to a request to access, exchange, or use EHI by providing the data elements in the USCDI for 24 months following the final rule's publication date.** Under the manner condition, an Actor must respond in the manner requested unless technically unable to respond or agreeable license terms cannot be reached, in which case it must respond in an alternative manner. *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 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.

Note, 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 fulfill the request at all, the Actor could seek coverage under the Infeasibility Exception.

Fees Exception — When will an Actor's practice of charging fees for accessing, exchanging, or using EHI not be considered information blocking?

Under the Fees Exception, Actors may recover certain costs reasonably incurred for the access, exchange, or use of EHI that HHS believes are unlikely to present information blocking concerns. Fees may result in a reasonable profit. The exception excludes certain fees, such as those based on electronic access to EHI by the individual. 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.

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. This exception will most likely be applicable to EHR vendors rather than physicians or other providers.

Licensing Exception — When will an actor's practice to license interoperability elements in order for EHI to be accessed, exchanged, or used not be considered information blocking?

According to the Licensing Exception, an Actor's practice to license interoperability elements for EHI to be accessed, exchanged, or used will not be considered information blocking if the practice meets certain timing

requirements and licensing conditions. The 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. Royalties and terms of the license also generally must be reasonable and non-discriminatory, in accordance with specified licensing conditions. *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.*

Info blocking may include interoperability element licensing practices or terms (e.g., royalties) with persons who require interoperability elements to develop or provide interoperable technologies or services.

- *Interoperability* element means hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that:
    - o May be necessary to access, exchange, or use EHI; and
    - o Is *controlled by the Actor*, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, or use of EHI.

The Licensing Exception seeks to balance an Actor's legitimate interest in protecting its intellectual property and earning a return on the investment with Cures' goal of interoperability and access, exchange and use of EHI. **This exception will most likely be applicable to EHR vendors rather than physicians or other providers.**