21st Century Cures

Act: Interoperability, Information Blocking, and the ONC Health IT Certification Final Rule

Summary of Information Blocking and Eight Exceptions

I. An Overview

The Law

The 21st Century Cures Act (Cures Act) was signed into law on December 13, 2016. Among the many health IT-related provisions it contains is one related to "Information Blocking" in Section 3022. There are penalties for non-compliance, some of which have not yet been outlined by federal authorities.

The Rule

On May 1, 2020, the Office of the National Coordinator for Health IT (ONC) published its final rule in the *Federal Register* addressing interoperability, information blocking and health IT certification requirements. These execute and deliver on requirements contained in the 21st Century Cures Act.

Please note there are several new acronyms and definitions which will have significant impacts on the healthcare industry. We have defined and explained them below.

Relevant citations to sections of the regulatory text and other additional explanatory information noting differences between the proposed and final rule are included in footnotes should readers require this information.

II. Definitions

What is information blocking?

Information blocking is a practice that is:

(1) likely to interfere with the access, exchange, and use of **electronic health information (EHI)** [defined below] except as required by law or covered by an exception; and

(2) conducted by a health IT developer, health information network or health information exchange that knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI; or

(3) conducted by a health care provider that knows that such practice is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

NOTES:

- **"Interfere with"** is inclusive of preventing and materially discouraging.

- The final rule defines “access,” "exchange," and “use.”
  - **“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 bi-directional 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, electronic health information (EHI), was established by Congress in the Cures Act; however, it was not defined in law. Rather, ONC has defined it in this rule. The final rule provides a more focused definition of 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.

Also for the first 24 months after publication of the final rule, EHI for the purposes of the information blocking definition is limited to the data elements represented in the US Core Data for Interoperability (USCDI) V1 standard adopted in the final rule.

What is NOT electronic health information (EHI)?

EHI does not include psychotherapy notes or information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding.

Health information that is deidentified consistent with the HIPAA regulations should not be included in the EHI definition. Once PHI has been de-identified, it is no longer considered PHI.

III. Compliance & Enforcement

Who must comply and when?

Congress names four types of entities they refer to as “actors” who must comply with information blocking requirements:

A. Health care providers;
B. Health IT developers of certified health IT; and
C. Health Information Networks (HINs) or Health Information Exchanges (HIEs) (HIN and HIE are combined into one defined type in final rule).

See our related cheat sheet for an overview of these three types of actors and how the Office of the National Coordinator for Health IT (ONC) defines them.[1] All actors must begin complying with the information blocking requirements in 45 CFR part 171 by November 2, 2020.

How will the information blocking provision be enforced and what are the penalties and disincentives for violations?

The Cures Act authorizes the U.S. Department of Health & Human Services' (HHS) Office of the Inspector General (OIG) to investigate claims of information blocking. The law calls for civil monetary penalties (CMPs) for Health IT Developers, HINs and HIEs of up to $1 million per violation. The OIG published a proposed rule in the *Federal Register* on April 24, 2020 with a 60-day comment period. This proposed rule provides more detail regarding information blocking enforcement and CMPs. At a minimum, the timeframe for enforcement would not begin sooner than the November 2, 2020 compliance date and depends on OIG's final rulemaking on the CMPs.

The CMPs do not apply to providers unless the provider meets the definition of HIN or HIE. If the OIG determines a provider has committed information blocking acting as a health care provider, the OIG will refer the provider to the appropriate agency to be subject to appropriate disincentives which will be addressed by the HHS Secretary through future notice and comment rulemaking.

When does a practice implicate the information blocking provision?

ONC, for the most part, referred readers to examples provided in the proposed rule of practices likely to interfere with access, use, and exchange of EHI and therefore implicate the information blocking provision. However, the final rule provides clarifications of concepts expressed in some of those examples for the following categories of practices:

A. 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).
B. 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).

[1] Our cheat sheet addressed who is covered under the definitions. For those interested in who is not covered ONC states on page 25803 of the rule, "the narrower definition of HIN/HIE in this final rule should clearly exclude entities that might have been included under the proposed definitions, such as social networks, internet service providers, and technology that solely facilitates the exchange of information among patients and family members. The definition in this final rule continues to focus on the functional activity of the individual or entity in question and not on any title or classification of the person or entity."

C. Impeding innovations or advancements in access, exchange or use of health-IT enabled care delivery such as refusing to license or allow the disclosure of interoperability elements to persons who require the elements to develop and provide interoperable technologies or services that might compete or complement an actor's own technology or services.
D. Rent seeking or other opportunistic pricing practices.
E. Non-standard implementation practices that lead to unnecessary complexity and burden, such as additional cost and effort required to maintain point-to-point connections, custom-built interfaces, and one-off trust agreements.

Third-Party Apps Used by Consumers

The final rule preamble specifically addressed the difference between an actor, such as a health care provider, *interfering with* versus *educating* when it comes to individuals choosing a third-party application that was developed and controlled by an individual or entity that is not covered by the HIPAA rules (e.g., is not a business associate with a BAA with the actor) and/or does not meet the definition of health IT developer of certified health IT.

The final rule supports and strongly encourages providing individuals with factual, unbiased information about the privacy and security practices of the app developer that will assist them in making the best choice for themselves in selecting a third-party app to access and receive all or part of their EHI from a health care provider. The final rule states that practices to educate individuals would not likely interfere with the access, exchange, and use of EHI if they meet certain criteria:

A. The information provided by the actor must focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology.
B. The information provided is factually accurate, unbiased, objective, and not unfair or deceptive.
C. The information is provided in a non-discriminatory manner (i.e., treat all third-party apps the same way in terms of whether or not information is provided to individuals).

Actors, may for example, establish processes where they notify a patient, call to a patient's attention, or display in advance – as part of an app authorization process with certified technology – whether the third-party developer of the app the patient is about to authorize to receive his/her EHI has attested in the positive or negative to whether the third party's privacy and security policies and practices meet certain "best practices" set by the market. To assist actors, the final rule suggests (but does not require) minimum criteria all third-party privacy policies and practices should adhere to. Note that after providing this information to an individual, the actor may not prevent the individual from deciding to use an app despite the risks noted regarding the app itself or the practices of the third-party developer.

The bottom line is that a practice that seemingly meets the statutory definition of information blocking above would not be information blocking if it is required by law, if one or more elements

of the definition are not met, or if it is covered by one or more of the eight exceptions established in the final rule and discussed below.

IV. Structure of Exceptions

The final rule clarified an actor 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 the information blocking provision and are tailored to align with the following criteria:

A. **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 .
B. **Address significant risk:** Each exception addresses a significant risk that actors would not engage in beneficial practices because of uncertainty about the breadth and applicability of the information blocking provision.
C. **Subject to strict conditions:** Each exception is subject to strict conditions to ensure practices are limited to those that are reasonable and necessary.

Failure to meet conditions of an exception does not mean a practice is information blocking, only that it would not have guaranteed protection from CMPs or disincentives, and would be evaluated on case-by-case basis (e.g., for level of impact, intent, knowledge).

The ONC retained the seven proposed exceptions in the final rule but revised them to provide clarity. ONC also established a new exception ("Content and Manner" exception) that will provide actors time to adjust to the new information blocking provisions and permit providers to deliver, at a minimum, a limited set of EHI comprised of the USCDI V1 data elements for access, exchange, and use during the 18 months after the information blocking compliance date. The new exception also provides an actor some alternatives in the manner used to fulfill a request for EHI if the manner requested is not technically feasible—such as alternative technical methods, standards (content and transport), or format. The actor can also fulfill a request in an alternative manner if the actor cannot reach agreeable terms with the requestor on fees and licensing for the manner requested.

ONC has also organized the exceptions under two categories (two subparts under the Part 171 of the regulation): those that involve not fulfilling requests and those that involve procedures for fulfilling requests to access, exchange, or use EHI.

Below are the final exceptions, a discussion of each, and sub-exceptions/conditions that need to be met for the exception to apply.

V. Summary of Eight Information Blocking Exceptions

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

A. **Preventing Harm Exception**
B. **Privacy Exception** (for this exception to apply, an actor must satisfy at least one of the sub-exceptions):
   1. **Pre-condition not satisfied** (relates to federal or state law requiring a precondition be met before sharing)
   2. **Developer not covered by HIPAA** (relates to when a health IT developer of certified health IT is not covered by the HIPAA Privacy Rule
   3. **Denying right to access** (relates to when a covered entity or business associate denies an individual's request for access to their ePHI)
   4. **Individual's request not to share** (relates to not providing access, exchange, or use of EHI pursuant to an individual's request)
C. **Security Exception**
D. **Infeasibility Exception**
E. **Health IT Performance Exception**

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

F. **Content and Manner Exception**
G. **Fee Exception**
H. **Licensing Exception**

VI. Summary of Each Information Blocking Exception Broken Down

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

A. Exception #1: 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 was finalized largely as proposed with modifications to better align with the HIPAA rules[2] to streamline compliance with the two regulations, particularly to reduce compliance burden and potential confusion for covered entities. ONC clarified the regulation text to make it easier to understand what the specific conditions of the Preventing Harm Exception are and how they relate to one another.

For the Preventing Harm Exception to apply, the following conditions must be met:

[2] The final rule's regulatory text was revised from the proposed rule to reflect more granular and comprehensive alignment of the type of harm condition with the harm standards in HIPAA section 164.524(a)(3).

1. *Reasonable belief the practice will substantially reduce the risk of harm.* An actor must hold a reasonable belief its practices are likely to or do interfere with otherwise permissible access, exchange, or use of EHI and that by not sharing information that this will substantially reduce the likelihood of harm to a patient (who is the subject of the EHI affected by the practice) or another person.

2. *Practice breadth.*
   The practice(s) implemented to substantially reduce the risk of harm must be no broader than necessary.

3. *An actor must also satisfy at least one condition from each of the categories described in a. b. and d. below and the condition described in c. if applicable:*

   a. *Type of risk. The types of risk of harm recognizable under the Risk of Harm Exception include risks:*

      - Arising from corrupt or inaccurate data being recorded or incorporated in a patient's EHI;
      - Arising from misidentification or mismatching a patient or patient's EHI; and
      - Identified by a licensed health care professional that a specific access or disclosure of EHI is reasonably likely to endanger the life or physical safety of the patient or another person.

      The final rule specifies the type of risk of harm must either:

      i. Be determined on an individualized basis by a licensed healthcare provider in the exercise of professional judgement. The provider must have a prior or current clinician-patient relationship with the patient whose EHI is affected by the determination; or
      ii. Arise from data known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous[3] for another reason.

      Note that if an actor lacks the technical capability to sequester only the subset of EHI the actor knows or reasonably suspects to be impacted by data issues giving rise to risk of harm, the Preventing Harm Exception will not recognize withholding the remaining EHI from access, use or exchange and refers actors to the Content and Manner and Infeasibility Exceptions.

[3] "Erroneous" replaced "inaccurate" in final rule and combined all data-specific sources of risk of harm in the final regulatory text.

b. Type of harm. Must be a harm that could serve as grounds for a covered entity to deny access to an individual's PHI pursuant to HIPAA under the:

i. Substantial harm standard where the practice is likely to or does interfere with access, use, or exchange of a patient's EHI by his/her legal representative (including personal representative as recognized in HIPAA) and the practice is implemented based on VI.A.3.a.i above.
ii. Substantial harm standard where the practice is likely to or does interfere with a patient's or his/her legal representative's access, use, or exchange of a patient's EHI that references another person and the practice is implemented based on VI.A.3.a.i above.
iii. Danger to life or physical safety harm standard where the practice is likely to or does interfere with a patient's access, use, or exchange of his/her EHI and the practice is implemented based on VI.A.3.a.i or VI.A.3.a.ii above; or
iv. Danger to life or physical safety harm standard where the practice is likely to or does interfere with a legally permissible access, use, or exchange of EHI not described in VI.A.3.b.i-iii above (for example, access, exchange, or use of EHI such as by health care providers furnishing services to the patient) and regardless of whether risk of harm the practice is implemented to substantially reduce is consistent with VI.A.3.a.i or VI.A.3.a.ii above.

c. Patient right to request review of individualized risk of harm determination

The actor must implement its 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, for determinations made consistent with VI.A.3.a.i above.

d. Practice implemented based on an organizational policy or a determination specific to the facts and circumstances

i. 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 Risk of Harm exception discussed above.
ii. Or in absence of an organizational policy (such as may be the case for some providers like solo or small practices that may not have comprehensive and formal policies), the practice must be based on a determination that relied on:
    1. Facts and circumstances known or reasonably believed at the time the determination is made and while the practice is in use; and
    2. Expertise relevant to implementing the practice consistent with the conditions in the Risk of Harm exception discussed above.

Even if an organizational policy exists, ONC understands it may be hard to anticipate all the potential risks of harm that could arise in real-world clinical or production environments of health IT. Therefore, in these circumstances, the actor could justify the practice or practices based on the particular facts and circumstances to show the practice is necessary and no broader than necessary to mitigate the risk of harm.

Documentation requirements

ONC did not specify a specific documentation requirement for licensed care providers when making an individualized determination of risk of harm for the determination risk to satisfy the risk of harm type condition finalized in the regulation for providers (VI.A.3.a.i above). ONC did not think it was necessary to require different or duplicate documentation of information that is already otherwise captured in the EHR or other reliable business records consistent with the HIPAA Privacy Rule and applicable state laws and that doing so would impose an unnecessary burden on providers. However, ONC did suggest that information relevant to determinations would include the facts or circumstances that substantially informed each determination, and any other decision-making information the provider may otherwise have difficulty recalling or reconstructing if later asked to explain how or why they reached an individualized determination in a particular case. ONC did confirm that documenting a determination in an EHR is considered an appropriate approach to document and retain documentation on determination of risk by a licensed health care provider.

B. Exception #2 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?

The Privacy Exception is structured to operate in a manner consistent with the framework of the HIPAA Privacy Rules with which covered entities and their business associates are already familiar. ONC finalized the sub-exceptions to the Privacy Exception to ensure individual privacy rights are not diminished as a consequence of the information blocking provision and to ensure the information 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 information blocking rule requires the actor to provide access, exchange, or use of EHI unless prohibited by law or covered by one of the exceptions.

In contrast to the other exceptions, this exception is structured with four discrete "sub-exceptions." An actor's practice must qualify for a sub-exception and the conditions of the sub-exception to be covered by the Privacy Exception. The sub-exceptions have, to a large

extent, been crafted to closely mirror privacy-protective practices presently recognized under federal and state privacy laws.

1. For the purposes of this exception only, the term "*individual"* in the final regulation text encompasses any or all of the following:

    a. An individual as defined by the HIPAA Privacy Rule;[4]
    b. A person who is the subject of EHI being accessed, exchanged, or used;
    c. A person who legally acts on behalf of the individual in a. or b. above in making health care-related decisions as a personal representative;[5]
    d. A person who is a legal representative of and can make health care decisions on behalf of an individual in a. or b. above; or
    e. An executor or administrator or other person having authority to act on behalf of a deceased person in a. or b. above or the individual's estate under state or other law.

2. *ONC finalized the four proposed sub-exceptions that address the following privacy protective practices in the final rule:*

    a. *Sub-exception 1: "Precondition not satisfied."*
    An actor will not be engaging in information blocking if the actor does not provide access, exchange, or use of EHI because a necessary precondition required by law is not satisfied.[6] This sub-exception will apply to all instances where an actor's ability to provide access, exchange, or use is "controlled" by a legal obligation to satisfy a condition, or multiple conditions, prior to providing that access, exchange, or use. The nature of the preconditions the actor must satisfy will depend on the laws that regulate the actor. For example, an actor regulated by a more restrictive state law may need to satisfy more preconditions than an actor regulated by less restrictive state laws.

    Examples that illustrate this sub-exception and would justify not providing access, exchange, or use of an individual's EHI:

    - Not being able to obtain consent of the individual required by certain federal and state laws for their EHI to be accessed, exchanged, or used for specific purposes, such as state laws requiring an individual's consent for uses and disclosure of EHI regarding sensitive health conditions, (i.e., HIV/AIDS, mental health, or genetic testing).

[4] 45 CFR 160.103
[5] In accord with 45 CFR 164.502 (g)
[6] The final rule deleted the word "privacy" when it refers to laws in the regulation text to alleviate ambiguity about what is meant by "privacy law."

- An individual's refusal to provide a HIPAA authorization required by law prior to providing access, exchange, or use of EHI.
- An actor is unable to verify the identity or authority of a person requesting access to EHI and such verification is required by law before providing access, exchange, or use of EHI.
- Another health care provider is requesting EHI for a quality improvement project that requires verification by the actor holding the information that the requestor has a relationship with the person whose information is being requested and the actor is unable to establish if the relationship exists.

The final rule suggests that an actor should carefully evaluate the state and federal law requirements imposed upon an actor and that the actor's responses are tailored to the legal precondition which protect and promote the privacy of EHI. ONC agreed that a precondition should be tailored to the applicable legal requirement and not to be tied only to a specific privacy risk or interest without a legally imposed requirement.

The actor must meet the following conditions to qualify for the *"Precondition not satisfied"* sub-exception:[7]

i. Practice must be implemented in a consistent and non-discriminatory manner.
ii. Organizational policies and procedures or case-by-case basis. An actor must document its organizational policies and specify the criteria used by the actor and, as applicable, the steps the actor will take to satisfy a precondition. Alternatively, if an actor's practice does not conform to an actor's policies and procedures, an actor must document on a case-by-case basis how it reached its decision including any pre-condition criteria that were not met and why.
iii. Precondition relies on a consent or authorization. If providing for the access, exchange or use of an individual's EHI requires the individual's consent or authorization, the actor must use reasonable efforts within its control to provide the individual with a consent or authorization form. If an actor receives some consent or an authorization form that requires the actor's assistance to satisfy missing elements that are not required by law and the actor does not provide the assistance, the actor may be engaged in information blocking.
iv. Did not improperly encourage or induce the individual to withhold consent or authorization. To the extent the precondition at issue was the provision of a consent or authorization by an individual, an actor must not have improperly encouraged or induced the individual to not provide her consent or authorization.
v. Multi-state actors subject to multiple laws with inconsistent preconditions. For purposes of determining whether a multi-state actor that is subject to multiple laws with varying and inconsistent preconditions has privacy policies and

[7] § 171.202.

procedures and actions that meet the organizational policies and procedures requirements and the preconditions that require consent or authorization requirements in the final rule shall be deemed to satisfy these requirements if the actor has adopted uniform policies and procedures (and does in fact apply them) to address the more restrictive preconditions.

b. *Sub-exception 2: "Health IT Developer of certified health IT not covered by HIPAA (referred to a non-covered actors)."*
Where a health IT developer of certified health IT offers a health IT product or service not regulated by the HIPAA Privacy Rule, the product or service is still subject to the information blocking provision. The rule enables non-covered actors under HIPAA that are actors under the information blocking provision to avail themselves of the Privacy Exception.

When engaging in a practice that promotes the privacy interests and interferes with access, exchange, and use of EHI, a non-covered actor must implement the practice according to a process described in its organizational privacy policies, disclose the policies to individuals and entities that use the actor's product or service before they agree to use the product or service, and the actor's privacy policies must: (1) comply with applicable state and federal laws; (2) be tailored to the specific privacy risk or interest being addressed; and (3) be implemented in a consistent and non-discriminatory manner to meet this sub-exception.

c. *Sub-exception 3: "Denial of an individual's request for his/her EHI in the circumstances provided in 45 CFR 164.524(a)(1) and (2)."*
This sub-exception permits a covered entity or business associate to deny an individual's request for access to their PHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) which applies to "unreviewable grounds" of access. This exception avoids a potential conflict between the HIPAA Privacy Rule and the information blocking provision.

Note that ONC clarified that if the same PHI that is subject of an access request is maintained in both the designated record set of the covered entity and that of the business associate, the PHI need only be produced once in response to a request for access.

d. *Sub-exception 4: "Respecting an individual's request not to share information."*
Individuals may have concerns about permitting their EHI to be accessed, exchanged, or used electronically under certain circumstances and request an actor to not share some or all of their EHI. This sub-exception would not apply if the actor is required by law to provide access, exchange, or use of EHI, such as when the

public interest in the disclosure of the individual's information outweighs the individual's interest in controlling the information (i.e., HIPAA required disclosures). Unless otherwise required by law, an actor can elect to not provide access, exchange, and use of an individual's EHI and qualify for this sub-exception if the following requirements are met:

i. The individual makes the request orally or in writing without any improper encouragement or inducement by the actor.
ii. The actor documents the request within a reasonable period of time. The final rule does not require a specific form of documentation and indicates a note in the certified EHR or similar notation is sufficient.
iii. If the actor terminates an individual's request for a restriction not to provide access, exchange, or use of the individual's EHI, the actor may only do so if the individual agrees to the termination in writing or requests the termination in writing; or the individual orally agrees to the termination and the actor documents the oral agreement; or the actor informs the individual it is terminating the agreement. The termination is not effective to the extent prohibited by law and is only applicable to EHI created or received after the actor informed the individual of the termination.

C. Exception #3 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?

The Security Exception permits actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain threshold conditions. Practices that purport to promote the security of EHI but are unreasonably broad, onerous on those seeking access to the EHI, are not applied consistently across/within an organization, or otherwise may unreasonably interfere with the access, exchange, or use of EHI would not qualify under this exception.

An actor's practice that is likely to interfere with the access, exchange, and use of EHI to protect the security of EHI will not be considered information blocking if the actor's practice meets the following conditions:

1. *The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.* Information that would support whether a practice meets this condition includes but is not limited to an actor's basis for adopting a particular security practice evidenced by the actor's organizational security policy, risk assessments the actor performed that informed the actor's security-based practice(s), and other relevant documentation an actor maintains, such as documentation maintained that supports meeting the HIPAA Security Rule.

2. *The practice must be tailored to the specific security practice addressed.* This condition presupposes an actor evaluated the risks posed by the security threat and developed a response tailored to mitigate the health IT or other related system vulnerabilities.

3. *The practice must be implemented in a consistent and non-discriminatory manner.* This condition should be understood to mean that similarly situated actors whose interactions pose the same level of security risk should be treated consistently with one another under the actor's security policies.

4. *For practices that implement an organizational security policy, the policy must:*
   a. Be in writing;
   b. Prepared on the basis of and be directly responsive to security risks identified and assessed by or on behalf of the actor;
   c. Align with one of more applicable consensus-based standards or best practice guidance; and
   d. Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

5. *For practices that don't implement an organizational security policy, an actor must have made a determination in each case based on the particular facts and circumstances that:*
   a. The practice is necessary to mitigate the security risk to EHI; and
   b. 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.

D. Exception #4 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 addresses certain circumstances that present legitimate practical challenges beyond an actor's control that may limit its ability to comply with requests 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.

ONC eliminated its proposed two-step test an actor would need to meet in order to demonstrate a request was infeasible and instead finalized a revised framework for this exception that provides two new conditions: *"Uncontrollable events"* and "*Segmentation*." Additionally, they revised the proposed *"Request is infeasible"* condition and now refer to it in the final regulatory text as *"Infeasible under the circumstances."*

They removed the *"Provision of a reasonable alternative"* condition from this exception and instead finalized it in the new Content and Manner Exception. If an actor was unable to meet the Content and Manner Exception, the actor could seek coverage under the Infeasibility Exception if the actor satisfied the *"Infeasible under the circumstances"* condition and responds to the requestor within 10 business days of the receipt of the request in writing with the reason(s) why the request is infeasible (i.e., *"Responding to requests*" condition). The final rule provides no specificity on the level of detail required in the written response.

To summarize, when the practice by an actor meets *one* of the *three* conditions detailed below, and the actor meets the requirements for responding to requests, the actor is not required to fulfill the request for access, exchange or use of EHI due to the infeasibility of the request.

1. *Uncontrollable events*:[8] The actor cannot fulfill a request for access, exchange, and use of EHI due to events beyond an actor's control, namely a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunications or internet service interruption, or act of military, civil or regulatory authority. Such events are all that is necessary to meet the infeasibility exception and no consideration of factors must be demonstrated or proven.

2. *Segmentation:*[9] An actor is not required to fulfill a request for access, exchange, or use of EHI if the actor cannot unambiguously segment the requested EHI from other EHI: (1) because of a patient's preference or because EHI cannot be made available by law; or (2) because the EHI is withheld in accordance with the Preventing Harm Exception.

3. *Infeasible under the circumstances*:[10] An actor demonstrates prior to responding to the requestor that the request would be infeasible under the circumstances. The rule requires the actor to do this through a written record or other documentation of its consideration of specified factors, applied in a consistent and non-discriminatory manner. The written record must be contemporaneous (i.e., the actor cannot use a post hoc rationalization claiming the request was infeasible under circumstances that were not considered at the time of the request).

   Factors the actor must consider and address in its determination: (Note the ONC removed three factors in the final rule):

[8] § 171.204(a)(1)
[9] § 171.204(a)(2)
[10] § 171.204(a)(3)

a. The type of EHI and the purposes for which it may be needed;
b. The cost to the actor of complying with the request in the manner requested;
c. The financial, technical, and other resources available to the actor;
d. Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
e. Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged;
f. Why the actor was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception in § 171.301.

Factors that the actor may not consider in its determination:

a. Whether the manner requested would have facilitated competition with the actor; and
b. Whether the manner requested prevented the actor from charging a fee or resulted in a reduced fee.

E. Exception #5 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?

ONC finalized the Health IT Performance Exception for certain practices an actor implements to maintain and improve the overall performance of health IT that are likely to interfere with the access, exchange, and use of EHI and will not be considered information blocking if certain conditions are met. The actor's practice will need to meet one of the conditions finalized in the rule for this exception as follows:

1. *Maintenance and improvements to health IT.* When an actor implements a practice that makes health IT under its control temporarily unavailable or temporarily degrades the performance of health IT to maintain or improve the health IT. The actor's practice:

   a. *Must be implemented for a period of time no longer than necessary to complete the maintenance or improvements that necessitated the unavailability or performance degradation of the health IT;*
   b. *Must be implemented in a consistent and non-discriminatory manner; and*
   c. *Must be consistent with existing service level agreements between the vendor and the individual or entity for planned or unplanned downtime or for unplanned downtime agreed to by the individual or entity.*

2. *Assured level of performance.* Establishes a condition expressly applicable to actions taken against a third-party application that is negatively impacting the health IT's performance. An actor must meet requirements for actions against a third-party application to qualify for this condition and be excepted from information blocking similar to the requirements above for the maintenance and improvements to health IT condition. The actor's practice must be:

    a. *For a period of time no longer than necessary to resolve impacts;*
    b. *Implemented in a consistent and non-discriminatory manner; and*
    c. *Consistent with existing service level agreements, if applicable.*

3. *Interaction with Preventing Harm and Promoting Security Exceptions.* When health IT is made unavailable for maintenance or improvements in response to risk of harm to a patient or another person or in response to a security risk to EHI, the actor must comply with the conditions specified in the those exceptions respectively in order to qualify for an exception to the information blocking provision.

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

F. Exception #6 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?

The Content and Manner Exception is a new exception finalized in the rule. It addresses two groups of comments from stakeholders: 1) those expressing concerns about the breadth of the proposed EHI definition and requesting implementation flexibility; and 2) those requesting clarification and improvement regarding the provision of "a reasonable alternative" in the proposed Infeasibility Exception. ONC removed the reasonable alternative provision in the Infeasibility Exception and finalized this new exception, which describes the content (i.e., the EHI) an actor is required to provide in responding to a request to access, exchange, or use EHI and the manner in which an actor must fulfill the request to satisfy this exception.

1. *Content condition:* The final rule narrowed the scope of EHI definition to ePHI to the extent it would be included in a designated record set (per HIPAA). For the first 24 months after publication of the final rule (until May 2, 2022), an actor must respond to requests for access, exchange, or use of EHI with, at a minimum, the EHI identified by the data elements in the USCDI standard adopted in the rule to meet the Content condition. After May 2, 2022, the actor's response to requests for access, exchange, or use of EHI must be in accord with the finalized EHI definition as described above.

2. *Manner condition.* To meet the Manner condition, an actor must fulfill a request for EHI described under the Content condition either 1) in the technical manner requested, referred to as *"any manner"* requested in the rule, unless technically unable (i.e., has technical limitations) to do so, or if unable to reach agreeable terms, such as technical terms, fees (market rates may be charged), and/or licensing of interoperability elements (IP to proprietary technology is not required to be licensed) or 2) in an *"alternative manner."*

   Under this condition, when responding in any manner requested, the fees charged and licensing of interoperability elements by the actor to fulfill the request are not required to satisfy the Fees Exception and/or the Licensing Exception, respectively. If the actor is not able to fulfill the request in any manner requested, the actor must fulfill the request in an alternative manner to satisfy the exception and must do so without unnecessary delay in the following priority order, starting with the first alternative below and only proceeding to the next if the actor is technically unable to fulfill the request in the manner identified:

   a. Using technology certified to standard(s) adopted in Part 170 *specified by the requestor;*
   b. Using content (structure – i.e., syntax – and terminology – i.e., semantics) and transport (method by which information is moved from one point to another) standards *specified by the requestor* and published by the federal government or a standards developing organization accredited by the American National Standards Institute (ANSI); and
   c. Using a mutually agreeable alternative machine-readable format, including the means to interpret the EHI.

   When responding to a request in an alternative manner, the fees charged and licensing of interoperability elements by the actor to fulfill the request are required to satisfy the Fees Exception and/or the Licensing Exception respectively.

   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.

G. Exception #7 Fees Exception—When will an actor's practice of charging fees for accessing, exchanging, or using EHI not be considered information blocking?

The Fees Exception is tailored to permit actors to set fees to recover costs reasonably incurred, including a reasonable profit margin, for access, exchange, or use of EHI and is

subject to strict conditions to prevent potential abuse, such as rent-seeking, opportunistic fees, and exclusionary practices that interfere with access, exchange, or use of EHI.

The Fees Exception only applies to fees charged for electronic access to EHI. *"Electronic access"* is specifically defined under this exception and means an internet-based method that makes the EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request. ONC emphasized an actor can charge fees to provide access to EHI through some other form of physical media, such as paper copies where EHI is printed out or where EHI is copied to a CD or flash drive. This would not be a practice that implicates the information blocking provision provided the fee(s) charged for that access comply with the HIPAA Privacy Rule. The rule does not limit fees and/or profits related to access, exchange, or use of information outside the scope of EHI. For the first 24 months after publication of the rule (until May 2, 2022), the fee conditions in this exception apply to just the limited EHI identified by the data elements represented in the USCDI standard.

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 the Conditions of Certification.

1. *Basis for fees condition*

    a. The fees an actor charges must be:
        i. Based on objective and verifiable criteria uniformly applied for all similarly situated persons and requests;
        ii. Reasonably related to the costs of providing access, exchange, or use to or at the request of the person or entity to whom the fee is charged;
        iii. Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied or for whom the technology is supported;[11] and
        iv. Based on costs not otherwise recovered for same instance of service to a provider and third party.[12]

    b. The fees an actor charges must not be based on:[13]

[11] The proposed language was changed to add *"similarly situated"* and change *"customers"* to *"persons."* ONC made these changes in response to comments received to allow, for example, sliding fee scales.
[12] New provision added in final rule.
[13] The ONC had proposed i. and iii. – v. under "excluded costs," but finalized them within the "Basis for fee condition" for clarity.

i. Whether requestor is a competitor, potential competitor, or will be using EHI in a way that facilitates competition with the actor;
ii. Sales, profit, revenue, or other value the requestor or other persons derive or may derive from the access, exchange, or use of the EHI.[14]
iii. Costs incurred due to a non-standard health IT design or implementation to access, exchange, or use EHI, unless requestor agreed to fees;
iv. Costs associated with intangible assets other than the actual development or acquisition costs of such assets;
v. Opportunity costs unrelated to access, exchange, or use of EHI; and
vi. Costs that led to the creation of intellectual property (IP), if the actor charged a royalty for that IP in accord with the Licensing Exception[15] and the royalty included development costs for IP creation.[16]

2. *Excluded fees condition.* ONC finalized under this condition the following proposed prohibited fees:

a. A fee prohibited by HIPAA under a patient's right to PHI.[17]
b. A fee based in any part on the electronic access[18] of an individual's EHI by the individual, personal representative, or another person or entity (e.g., third-party consumer-facing app) designated [authorized] by the individual.
c. A fee to perform an export of EHI via health IT certified to the EHI export criteria[19] for purposes of switching health IT products or to provide patients their EHI.
d. A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

3. *Compliance with the Condition of Certification condition.* Health IT developers of certified health IT subject to the Condition of Certification[20] are also required to comply with the requirements of this condition for all practices at all relevant times to qualify for the Fees Exception[21].

[14] While ONC removed "including secondary use of such information" from the regulatory text, the intent of this text remains with regards to secondary use of EHI.
[15] § 171.303
[16] New provision added in final rule.
[17] 45 CFR 164.524(c)(4)
[18] Meaning clarified and definition codified in § 171.302(d).
[19] § 170.315(b)(10)
[20] § 170.402(a)(4), § 170.404 or both.
[21] For clarity, ONC modified this condition in the final rule to remove the second proposed provision under this condition regarding a health care provider that acts as an API data provider because not all of the permitted fees in the API Condition of Certification (§ 170.404) are applicable for API data providers.

H. Exception #8 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?

In response to comments, ONC made several updates to the Licensing Exception as well as to terms and concepts that apply broadly to the information blocking provision.[22] Actors will need to assess their existing licensing contracts or agreements and make any necessary amendments to come into compliance with the information blocking provision by November 2, 2020.

The final rule finalized the following conditions under the Licensing Exception and an actor's practice will need to meet all the conditions to qualify for this exception:

1. *Negotiating a license condition.* Upon receiving a request to license an interoperability element for the access, exchange or use of EHI, the actor must begin license negotiations with the requestor within 10 business days from receipt of the request and negotiate a license with the requestor in good faith within 30 days from receipt of the request subject to the *Licensing conditions* in the rule. ONC suggested that in instances where an actor is unable to negotiate a good faith license within 30 days, the actor may not meet the conditions of this exception. As part of an information blocking investigation, ONC stated that the ONC and OIG may consider documentation or other writings maintained by the actor around the time of the license request that indicate why the actor was unable to meet the condition. While documentation is not required, this is highly suggestive that the actor should document these instances.

2. *Licensing conditions.* ONC removed references to "RAND" in the licensing conditions but finalized the majority of substantive conditions for licensing interoperability elements under this exception as proposed with slight modifications:

    a. *Scope of rights.*[23] ONC finalized the "scope of rights" which states the license must provide all rights necessary to: (1) enable the access, exchange, or use of EHI; and (2) achieve the intended access, exchange, or use of EHI via the interoperability element.

[22] ONC (1) revised the definition of interoperability elements; (2) clarified that if there is no nexus between a requestor's need to license an interoperability element and existing EHI on one or more patients, an actor does not need to consider licensing the interoperability requested; (3) clarified the process and timeframe for negotiating a license; (4) removed the "reasonable and non-discriminatory" or "RAND" framework; and (5) clarified the relationship between this exceptions and the Fees Exception.
[23] ONC replaced the rights proposed in the "scope of rights" to more clearly and succinctly explain what they were trying to convey in the Proposed Rule.

b. *Reasonable royalty.* ONC proposed that if an actor charges a royalty for the use of interoperability elements, the royalty base and rate must be reasonable. They proposed and finalized that the reasonableness of any royalties would be based solely on the basis of the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information. In evaluating the actor's assertions and evidence that the royalty was reasonable, ONC proposed and reiterated in the final rule that they may consider the following factors:

- The royalties received by the actor for the licensing of the proprietary elements in other circumstances comparable to RAND-licensing circumstances.
- The rates paid by the licensee for the use of other comparable proprietary elements.
- The nature and scope of the license.
- The effect of the proprietary elements in promoting sales of other products of the licensee and the licensor, taking into account only the contribution of the elements themselves and not of the enhanced interoperability that they enable.
- The utility and advantages of the actor's interoperability element over the existing technology, if any, that had been used to achieve a similar level of access, exchange, or use of EHI.
- The contribution of the elements to the technical capabilities of the licensee's products, taking into account only the value of the elements themselves and not the enhanced interoperability that they enable.
- The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the proprietary elements or analogous elements that are also covered by RAND commitments.
- The portion of the realizable profit that should be credited to the proprietary elements as distinguished from non-proprietary elements, the manufacturing process, business risks, significant features or improvements added by the licensee, or the strategic value resulting from the network effects, switching costs, or other effects of the adoption of the actor's technology.
- The opinion testimony of qualified experts.
- The amount that a licensor and a licensee would have agreed upon (at the time the licensee began using the elements) if both were considering the RAND obligation under this exception and its purposes, and had they reasonably and voluntarily trying to reach an agreement.

ONC finalized the "Reasonable royalty" regulatory text as proposed with a slight modification to § 171.303(c)(2)(iii) for consistency. This new paragraph states an

actor may not charge a royalty for IP if the actor recovered any development costs pursuant to § 171.302 (i.e., the Fees Exception) that led to the creation of the IP.

c. *Non-discriminatory terms.* ONC finalized that the terms on which an actor licenses and otherwise provides interoperability elements must be non-discriminatory. This requirement would apply to both price and non-price terms, and thus would apply to the royalty terms discussed immediately above as well as other types of terms that may be included in licensing agreements or other agreements related to the provision or use of interoperability elements.

To comply with this condition, the terms on which the actor licensed the interoperability elements must be based on objective and verifiable criteria that the actor applied uniformly for all similarly situated classes of persons and requests. ONC made a slight modification to § 171.303(c)(3)(i) and removed "substantially similar" from the text.

Also, the terms must not be based on whether the requestor is a competitor or potential competitor, or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor. Nor can the terms be based on revenue or other value the requestor may derive from access, exchange, or use of EHI obtained via the interoperability elements.

d. *Collateral terms.* ONC proposed and finalized five additional conditions that would reinforce the requirements of this exception discussed above. First, the actor must not require the licensee or its agents or contractors to not compete with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development. Second, and for similar reasons, the actor must not require the licensee or its agents or contractors to deal exclusively with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development. Third, the actor must not require the licensee or its agents or contractors to obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements. Fourth, the actor must not condition the use of interoperability elements on a requirement or agreement to license, grant, assign, or transfer the licensee's own IP to the actor. Finally, the actor must not condition the use of interoperability elements on a requirement or agreement to pay a fee of any kind whatsoever unless the fee meets either the narrowly crafted condition to this exception for a reasonable royalty, or, alternatively, the fee satisfies the requirements in the Fee Exception, which permits the recovery of certain costs reasonably incurred.

e. *Non-disclosure agreements.* ONC proposed and finalized that an actor would be permitted under this exception to require a licensee to agree to a confidentiality or non-disclosure agreement (NDA) to protect the actor's trade secrets, provided that the NDA is no broader than necessary to prevent the unauthorized disclosure of the actor's trade secrets. Further, ONC proposed and finalized that the actor would have to identify in the NDA the specific information that it claims as trade secrets, and that such information would have to meet definition of a trade secret under applicable law.

f. *Additional conditions relating to the provision of interoperability elements.* ONC proposed and finalized that an actor would not qualify for this exception if it engaged in a practice that had the purpose or effect of impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose; or of impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

   To ensure the actor's commitments under this exception are durable, ONC proposed and finalized one additional safeguard: An actor cannot avail itself of this exception if, having licensed the interoperability elements, the actor degrades the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

g. *Compliance with Condition of Certification.* ONC removed this condition for consistency with other exceptions for clarity, as condition is not necessary.

NOTE:

The final rule advises that actors should assess their policies and practices related to verifying the identity of patient, or a legal representative of a patient for consistency with the finalized Privacy and Security exceptions. Actor should also assess its policies and practices implemented to confirm a representative's legal authority to access or request or authorize access, exchange, and use of a minor's EHI on behalf of a minor information in context of the finalized Privacy and Security Exceptions. In cases where otherwise applicable law prohibits a specific access, exchange, or use of information, an exception to Part 171 is not necessary due to the exclusion of "required by law" practices from the statutory information blocking definition. Where access and exchange is permissible by law and an actor simply lacks the technical capability to provide access, exchange, or use in a specific requested mechanism, format, or manner, the actor should review its policies and practices for consistency with the Content and Manner or Infeasibility Exceptions in the final rule.


CHiME
PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON