



Clinical Connections: Interoperability Intensive for Health Plans

Session 3: What are Information Blocking Exceptions and How Should I Use Them?

October 20, 2021



THANK YOU

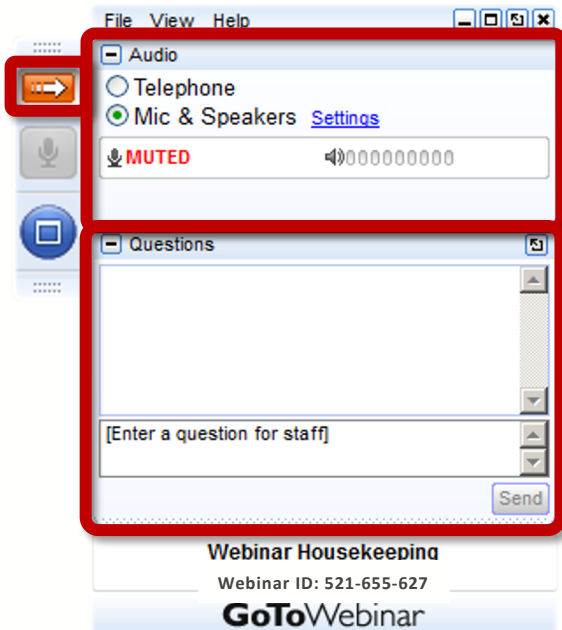
TO OUR CLINICAL CONNECTIONS SPONSORS



An association of independent Blue Cross and Blue Shield companies



How to Participate



Your Participation

Open and close your control panel

Join audio:

- Choose "Mic & Speakers" to use VoIP
- Choose "Telephone" and dial using the information provided

Submit questions and comments via the Questions panel

Note: Today's presentation is being recorded and will be provided

Problems or Questions? Contact the Interoperability Matters Team at:

interopmatters@sequoiaproject.org

Intensive Goal and Objectives: Why Participate

Goal

The Interoperability Intensive will provide carefully vetted, substantive resources and relevant information for health plans about requirements of the ONC Information Blocking regulations and related CMS interoperability and clinical data rules, with a focus on enhancing health plans' relationships with providers and effective responses to resulting opportunities and requirements.

Objectives

1. Provide in-depth study of the Cures Act and the ONC and OIG Information Blocking rules, focusing on implications for health plan clinical data access, including which organizations are Actors, prohibited practices, key definitions, regulatory exceptions, and penalties/ "disincentives."
2. Summarize key elements of CMS interoperability and clinical data access rules and linkages to ONC rules and programs.
3. Deliver practical and useful guidance and tools to help participants design and implement plans for their organizations to navigate the new regulatory and data access landscape.
4. Promote information sharing among participants during and after sessions.
5. Create a *Community of Interest* to encourage participants to continue sharing learnings and best practices after the Intensive concludes.

Meet The Sequoia Project Team



Mariann Yeager
CEO
The Sequoia Project



Steve Gravely
Founder & CEO
Gravely Group



Mark Segal
Principal
Digital Health Policy Advisors

About the Sequoia Project

The Sequoia Project is the independent, trusted advocate for nationwide health information exchange. In the public interest we steward current programs, incubate new initiatives, each with their own mission, governance, membership and structure, and educate our community.



SECURE



INTEROPERABLE



NATIONWIDE

Clinical Connections: Interoperability Intensive Sessions

Between 3pm and 5pm ET on the following dates:

- | | |
|--|-------------------|
| 1. Overview | October 6, 2021 |
| 2. What is an Information Blocking Violation? | October 13, 2021 |
| 3. Exceptions: Part 1 | October 20, 2021 |
| 4. Exceptions: Part 2 | October 27, 2021 |
| 5. CMS Rules | November 3, 2021 |
| 6. Enforcement Issues | November 10, 2021 |
| 7. Compliance, Organizing for Success, and Wrap-Up | November 17, 2021 |

Clinical Connections: Interoperability Intensive Office Hours

Between 2pm and 3pm ET on the following dates:

1. October 7, 2021
2. October 14, 2021
3. October 21, 2021
4. October 28, 2021
5. November 4, 2021
6. November 15, 2021
7. November 18, 2021

Interoperability Intensive Materials

We have developed materials for you to use as part of the Intensive. These supplement, but do not replace, Intensive sessions.

- *Information Blocking Summary*—an extensive narrative that provides a comprehensive discussion of:
 - The legal authority for Information Blocking in the CURES Act, the ONC Final Rule, and the OIG Proposed Rule;
 - Key definitions and the exceptions.
- *Compliance Planning Workbook*—a comprehensive discussion of organizational compliance and implementation for Information Blocking with checklists, examples and suggestions.

Clinical Connections: A 7-Week Interoperability Intensive
Welcoming Health Plans and Their Partners

Access materials and forum as part of the Intensive. After completing the Intensive, should you choose to join The Sequoia Project, you will have continued access to the intensive site and its materials, including the forums and future discussions.

VIEW CLASSROOM >

Upcoming Sessions/Office Hours
Download calendar invite (.ics)

06 October 2021
Clinical Connections Session
Find out more >

Recent Forum Topics

Welcome to Clinical Connections: A 7-Week Interoperability Intensive

VIEW ALL TOPICS >

Boot Camp Sponsors and Benefits
Members of Blue Cross Blue Shield Companies, UnitedHealthcare, and Da Vinci Project receive:

United Healthcare BlueCross BlueShield Association DA VINCI

- A limited-time 25% The Sequoia Project membership discount for first year, in addition to applying Clinical Connections intensive fees paid;
- One additional dedicated office hour call with the experts; and
- Extended access to course materials and recordings.

<https://sequoiaproject.org/2021-clinical-connections/>

Certificate of Participation

- Sequoia has invested extensive resources into this Clinical Connections: Interoperability Intensive to provide participants with an excellent orientation to Information Blocking and clinical interoperability
- The core faculty, Steve Gravely and Mark Segal, are experts on the Information Blocking and clinical interoperability provisions
- The written materials have been carefully vetted for accuracy and objectivity
- Each session will include vital information and time for group discussion
- Participants are encouraged to share ideas and information outside of the Intensive sessions
- All participants that attend each Intensive session will receive a **Certificate of Completion** as tangible evidence of their achievement



Quick Refresher-Practices

- Practices can be an **act or an omission** by an actor
- ONC identified many specific examples of practices in the Proposed and Final Rule but these are illustrative only and **NOT** exhaustive
- Practices can be anything that interferes with access, exchange or use of EHI
- A practice is not an automatic information blocking violation, an Actor must have the **required knowledge or intent** to interfere with access, exchange or use of EHI
- The practice must not fall within an exception or otherwise be required by law
- Understanding practices is essential for health plans and other data requesters



Session 3: Exceptions – Part 1

Session Goals

- This initial session on Exceptions will be an overview of the way ONC organizes exceptions in the Final Rule, and what we can infer from changes made in the Final Rule
- We will review the role of the elements to each exception and what it means to meet an exception and document compliance
- We will also begin detailed review of the Preventing Harm, Privacy, Security, and Health IT Performance Exceptions
- This discussion will emphasize implications and strategies for health plans and other data requesters



Exceptions: An Overview

What is the Legal Basis for the Exceptions?

- “Exception” is a term in definition of Information Blocking in the ONC Final Rule to implement a concept in the Cures definition of Information Blocking
- Congress directed ONC to identify activities that were “reasonable and necessary” to achieve a greater public purpose despite the likelihood that the practice would be information blocking
- Cures (Section 4004)
*A practice by a health care provider, health IT developer, health information exchange, or health information network that, except as required by law **or specified by the Secretary as a reasonable and necessary activity**, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information*
- ONC Final Rule (§ 171.103 Information blocking)
*(a) Information blocking means a practice that—
(1) Except as required by law **or covered by an exception** set forth in subpart B or subpart C of this part, is likely to interfere with access, exchange, or use of electronic health information*

Finalized Exceptions and their Role

- Responding to comments, in the Final Rule ONC revised the proposed exceptions, added an eighth exception, provided guidance and examples, and divided the exceptions into two categories:
 1. Not fulfilling requests to access, exchange, or use EHI
 2. Procedures for fulfilling requests to access, exchange, or use EHI
- ONC changed the titles of each exception into a question format to reinforce that each exception includes practices likely to interfere with the access, exchange or use of EHI
- Many **documentation requirements** are embedded in exception conditions; in all cases, **documentation of how exception conditions are met will be essential**
- **Failing 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., level of impact, intent, knowledge)**

Exceptions: ONC FAQ (1)

Q: If an actor does not fulfill a request for access, exchange, and use of EHI in “any manner requested” that they have the technical capability to support, is the actor automatically an information blocker unless they satisfy at least one of the information blocking exceptions?

- Not necessarily. The [eight information blocking exceptions](#) defined in 45 CFR part 171 are voluntary and offer [actors](#) certainty that any practice meeting the conditions of one or more exceptions will not be considered information blocking. However, an actor’s practice that does not meet the conditions of an exception will not automatically constitute information blocking. Instead such practices will be evaluated on a case-by-case basis to determine whether information blocking has occurred.
- Whether information blocking occurred in a particular case would be based on whether:
 - the individual or entity engaging in the practice is [an "actor"](#) as defined in 45 CFR 171.102;
 - the claim involves "EHI" as defined in 45 CFR 171.102;
 - the practice was required by law;
 - the actor's practice met the conditions of [an exception under 45 CFR 171](#);
 - the practice rose to the level of an interference under 45 CFR 171; and,
 - the actor met the requisite knowledge standard.

Exceptions: ONC FAQ (2)

- Please note, the knowledge standard varies based on the type of actor.
 - For health care providers, the standard is that the actor “knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.”
 - For health IT developers of certified health IT and health information networks (HINs) or health information exchanges (HIEs) the standard is that the actor “knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.” In addition, we recommend review of the examples included in the Final Rule of what is and is not considered [interference at 85 FR 25811](#).

What Eight Exceptions are Identified by ONC?

Not Fulfilling Requests to Access, Exchange, or Use EHI

1. Preventing Harm
2. Privacy
3. Security
4. Infeasibility
5. Health IT Performance

Procedures for Fulfilling Requests to Access, Exchange, or Use EHI

6. Content and Manner
7. Fees
8. Licensing

How Do Actors Use Exceptions?

- Exceptions are an affirmative defense to a claim that a practice is information blocking
- Burden is on an actor to demonstrate that its practice meets an exception
 - Actors cannot simply assert an exception and require the OIG to prove that they don't meet it
- Actor must prove it meets **every element** of the exception(s) that it is asserting
- **Actors are likely to use/cite/document exceptions in dealings with data requesters**

Handling Exceptions: Actors and Data Requesters

- Using exceptions effectively will require a **plan, careful documentation, coordination, and accountability**
- Each exception will involve **team members from across an actor and data requester organization**; see examples in *Compliance Planning Workbook*
- Exceptions will often be **sequenced strategically** (e.g., Content and Manner before Fees, Licensing, or Infeasibility)
- Some exceptions have a **“time clock”** in which they must be claimed or elements applied (e.g., response to an inquiry)
- Exceptions very relevant for **framing data requests**, for responses to requests and with enforcement agencies



Exceptions: Part 1

Preventing Harm Exception (1)

- An actor may engage in practices that are **reasonable and necessary** to **prevent harm** to a patient or another person
- The actor must have a **reasonable belief** the practice will substantially reduce the likelihood of harm to a patient or another person
- The **type of harm** being prevented must be harm that a HIPAA covered entity could use to deny access to an individual's PHI under the Privacy Rule's Right of Access (45 CFR 162.524 (a)(3))
 - Access requested is “reasonably likely to **endanger the life or physical safety**” of the individual or another person (45 CFR 162.524 (a)(3)(1)) **IF** the practice affects the individual's access, exchange or use of their own PHI **or the legally permissible request is not otherwise covered in the first three conditions (e.g., provider or health plan request)**
 - Access requested is “**reasonably likely to cause substantial harm** to another person” if the PHI references another person
 - Access is “reasonably likely to cause substantial harm to the individual or another person” if requested by the individual's legal representative

Preventing Harm Exception (2)

- Except for requests from individual or “other” category, **risk of harm** must:
 - be determined on an **individualized basis** in the exercise of **professional judgment** by a **licensed health care professional** who has a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination; **OR**
 - arise from data known or reasonably suspected to be **misidentified or mismatched, corrupt** due to technical failure, or **erroneous** for another reason
- The practice must be **no broader than necessary** to substantially reduce the risk of harm that the practice is implemented to reduce
- Must based on either:
 - an **organizational policy** that is in writing, based on relevant clinical, technical and other appropriate expertise and implemented in a consistent and non-discriminatory manner; **OR**
 - **individualized determination** based on facts/circumstances known or reasonably believed at the time and relevant expertise

Preventing Harm Exception: ONC FAQ

Question: Would the Preventing Harm Exception cover a “blanket” several day delay on the release of laboratory or other test results to patients so an ordering clinician can evaluate each result for potential risk of harm associated with the release?

Answer: No. Blanket delays that affect a broad array of routine results do not qualify for the Preventing Harm Exception. The Preventing Harm Exception is designed to cover only those practices that are no broader than necessary to reduce a risk of harm to the patient or another person.

As we discussed in the Cures Act Final Rule, a clinician generally orders tests in the context of a clinician-patient relationship. In the context of that relationship, the clinician ordering a particular test would know the range of results that could be returned and could prospectively formulate, in the exercise of their professional judgment, an individualized determination for the specific patient that:

- withholding the results of the particular test(s) from the patient would substantially reduce a risk to the patient’s or another person’s life or physical safety – or –
- that withholding the results of the particular test(s) from a representative of the patient would substantially reduce a risk of substantial harm to the patient or another person.

Such individualized determinations made in good faith by an ordering clinician, in the exercise of their professional judgment and in the context of the treatment relationship within which they order the test, would satisfy the type of risk and type of harm conditions of the Preventing Harm Exception. Actors, including but not limited to the ordering clinician, could implement practices in reliance on such determinations and the Preventing Harm Exception would cover such practices so long as the practices also satisfy the other four conditions of the exception.

Privacy Exception (1)

- An actor may refuse to fulfill a request to access, exchange or use EHI **to protect an individual's privacy**
- This exception is unique because it contains **four sub-exceptions**, each with its own requirements:
 1. Preconditions prescribed by laws are not satisfied (e.g., required consent);
 2. Health IT developer of certified health IT is not covered by HIPAA (i.e., developer that is not a BA for a patient facing product or service) but that implement documented and transparent privacy policies;
 3. Denial of an individual's request for their electronic protected health information in the circumstances provided in [45 CFR 164.524\(a\)\(1\) and \(2\)](#) (unreviewable grounds for denying patient right of access); or
 4. Respecting an individual's request not to share information
- An actor must meet all the elements of **at least one** sub-exception
- Note: "Individual" is defined more broadly than in HIPAA to include others who have the legal authority to act on behalf of a patient such as spouse

Privacy Exception (2)

- Sub-exception #1 – Precondition not satisfied
 - Precondition must be **required by law or regulation**; ONC expressed concern that this sub-exception not be used as a “pretext” to refuse to fulfill a request
 - Actor’s privacy-protective practices must be based on **objective criteria** that are applied uniformly for all substantially similar privacy risks
 - Practices must be **tailored** to the specific privacy risk and the legal pre-condition (e.g., identity verification)

Privacy Exception (3)

- Sub-exception #2– Health IT developer not covered by HIPAA
 - Does **not** apply if health IT developer is a business associate of a Covered Entity
 - Would apply to health IT developer of certified health IT involved in only direct-to-consumer products or services
 - Practice **must** be described in detail in actor’s privacy policy (e.g., blanket requirement of customer consent not valid absent rationale for why prior consent is necessary)
 - Practice **must** be disclosed in advance in plain language
 - Practice must be tailored

Privacy Exception (4)

- Sub-exception #3 – Patient right of access
 - Limited to the “unreviewable” grounds for denying access to PHI under the HIPAA Privacy Rule (45 CFR 162.524 (A)(1) and (2))
 - Requests by inmates of correctional institution
 - Requests by individual participants in focused study while study in process
 - Records subject to the Privacy Act (5 USC 552a) if disclosure is prohibited
 - Information from non-healthcare provider under a promise of confidentiality
 - Psychotherapy notes
 - Information compiled in reasonable anticipation of, or in use in, civil, criminal or administrative action or procedure
 - Proposed Rule included “reviewable” grounds under HIPAA but those are now covered by Preventing Harm exception

Privacy Exception (5)

- Sub-exception #4 – Respecting individual’s request to not share information
 - Allows actors to respect an individual’s privacy choices without fear of information blocking
 - Request must come from the individual, be documented by the actor and implemented in a consistent, non-discriminatory manner
 - No interference or pressure on the individual to make the request

Privacy Exception (6)

- Actors need not provide access, exchange, or use of EHI in a manner **not permitted** under the [HIPAA Privacy Rule](#)
- Actors operating in **multiple states** can rely on an organizational policy that adopts the most stringent state law for the entire organization
- ONC emphasizes that information blocking provision **may require actors to provide access, exchange, or use of EHI in situations where HIPAA would not require access** of similar information (e.g., HIPAA Privacy Rule **permits, but does not require**, covered entities to disclose ePHI in most situations)

Security Exception (1)

- An actor may engage in a practice that is likely to interfere with the access, exchange or use of EHI to **promote security of EHI** provided the practice is:
 - **Directly related to safeguarding** confidentiality, integrity, and availability of EHI
 - **Tailored** to specific security risks being addressed
 - Implemented in a **consistent and non-discriminatory manner**
 - **If implementing an organizational security policy it must:**
 - Be in writing
 - Prepared for/be directly responsive to security risks identified by actor
 - Align with consensus-based standards/best practices
 - Provide objective timeframes/other parameters for identifying, responding to and addresses security incidents
 - If not implementing an organizational security policy, the practice must be based on specific facts and circumstances that the practice is necessary to mitigate risks and there is no reasonable alternative

Security Exception (2)

- ONC uses a **fact-based approach** to allow each actor to implement policies, procedures, and technologies **appropriate for its size, structure,** and **risks** to individuals' EHI
- The **intent is to prohibit practices** that “purport to promote the security of EHI but that are **unreasonably broad and onerous** on those seeking access to EHI, **not applied consistently** across or within an organization, or otherwise may **unreasonably interfere** with access, exchange, or use of EHI”
- Would apply to **security practices exceeding minimum HIPAA Security conditions**

Health IT Performance Exception (1)

- An actor's practices to maintain or improve health IT performance, even if those practices are likely to interfere with access, exchange or use of EHI are permitted under strict conditions
- For maintenance or improvements to health IT that make the health IT temporarily unavailable or temporarily degraded if:
 - The interruption lasts no longer than necessary, ONC said adopting specific timeframes was not practical
 - **Implemented in a fair and consistent manner**
 - **"Planned" interruptions must be consistent with existing SLAs**
 - "Unplanned" interruptions must be consistent with existing SLAs or agreed to
- Obligations differ if the Actor is a health IT developer or a provider
- ONC notes that a period of health IT unavailability or performance degradation could be within the parameters of the SLA but "longer than necessary" and potentially information blocking or conversely outside the parameters of the SLA without being "longer than necessary" and, therefore, without necessarily being information blocking **[Likely becomes a case-by-case issue]**

Health IT Performance Exception (2)

- An actor **may take action against a third-party application** (including but not limited to patient-facing apps) that is **negatively impacting the health IT's performance**, provided that the practice is—(1) For a period of **time no longer than necessary to resolve any negative impacts**; (2) Implemented in a **consistent and non-discriminatory manner**; and (3) **Consistent with existing SLAs**, where applicable
- **Harm, Security, or Infeasibility (e.g., disaster)-related practices** are addressed by or must also be consistent with those exceptions
- **Document the SLA or case-by-case factors** given exception criteria



Discussion



Coming Up In The Next Session

Session 4: Exceptions—Part 2

- We will make a detailed review of the remaining exceptions: including Infeasibility, Content and Manner, Fees, and Licensing
- We will also address exception interactions and sequencing

Interoperability Matters

<https://sequoiaproject.org/interoperability-matters/>

Appendix: Regulatory Language

§ 171.201 Preventing Harm Exception — When will an actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking? (1)

An actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm will not be considered information blocking when the practice meets the conditions in paragraphs (a) and (b) of this section, **satisfies at least one condition (subparagraph) from each of paragraphs (c), (d) and (f) of this section, and also meets the condition in paragraph (e) of this section when applicable.**

(a) *Reasonable belief.* The actor engaging in the practice must hold a **reasonable belief** that the practice will **substantially reduce a risk of harm** to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information affected by the practice. For purposes of this section, “patient” means a natural person who is the subject of the electronic health information affected by the practice.

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

(c) *Type of risk.* The risk of harm must:

(1) Be **determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship** with the patient whose EHI is affected by the determination; **or**

(2) **Arise from data that is known or reasonably suspected** to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

§ 171.201 Preventing Harm Exception — When will an actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking? (2)

(d) *Type of harm.* The **type of harm must be one that could serve as grounds for a covered entity (as defined in § 160.103 of this title) to deny access** (as the term “access” is used in part 164 of this title) to an individual’s protected health information under:

- (1) Section [164.524\(a\)\(3\)\(iii\)](#) of this title where the practice is likely to, or in fact does, interfere with **access, exchange, or use** (as these terms are defined in [§ 171.102](#)) of the patient’s EHI by their **legal representative** (including but not limited to personal representatives recognized pursuant to [45 CFR 164.502](#)) and the practice is implemented pursuant to an individualized determination of risk of harm consistent with (c)(1) of this section;
- (2) Section [164.524\(a\)\(3\)\(ii\)](#) of this title where the practice is likely to, or in fact does, interfere with the **patient’s or their legal representative’s access to, use or exchange** (as these terms are defined in § 171.102) of information that references another natural person and the practice is implemented pursuant to an individualized determination of risk of harm consistent with paragraph (c)(1) of this section;
- (3) Section [164.524\(a\)\(3\)\(i\)](#) of this title where the practice is likely to, or in fact does, interfere with the **patient’s access, exchange, or use** (as these terms are defined in § 171.102) of their own EHI, **regardless of whether the risk of harm that the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (c)(2)** of this section; **or**
- (4) Section [164.524\(a\)\(3\)\(i\)](#) of this title where the practice is likely to, or in fact does, interfere with a legally permissible access, exchange, or use (as these terms are defined in § 171.102) of electronic health information not described in paragraph (d)(1), (2), or (3) of this section, and **regardless of whether the risk of harm the practice is implemented to substantially reduce is consistent with paragraph (c)(1) or (2)** of this section.

§ 171.201 Preventing Harm Exception — When will an actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking? (3)

(e) Patient right to request review of individualized determination of risk of harm.

Where the risk of harm is **consistent with paragraph (c)(1)** of this section, the actor must implement the practice in a manner consistent with any rights the individual patient whose electronic health information is affected **may have under § 164.524(a)(4) of this title, or any Federal, State, or tribal law, to have the determination reviewed and potentially reversed.**

§ 171.201 Preventing Harm Exception — When will an actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to prevent harm not be considered information blocking? (4)

(f) *Practice implemented based on an **organizational policy** or a **determination specific to the facts and circumstances**.* The practice must be consistent with an organizational policy that meets paragraph (f)(1) of this section or, in the absence of an organizational policy applicable to the practice or to its use in particular circumstances, the practice must be based on a determination that meets paragraph (f)(2) of this section.

(1) An **organizational policy must:**

(i) **Be in writing;**

(ii) **Be based on relevant clinical, technical, and other appropriate expertise;**

(iii) **Be implemented in a consistent and non-discriminatory manner;** and

(iv) **Conform each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use.**

(2) A **determination must:**

(i) **Be based on facts and circumstances known or reasonably believed by the actor** at the time the determination was made and while the practice remains in use; **and**

(ii) **Be based on expertise relevant to implementing the practice consistent with the conditions** in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use in particular circumstances.

§ 171.202 Privacy Exception — When will an actor’s practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual’s privacy not be considered information blocking? (1)

An actor’s practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual’s privacy will not be considered information blocking when the **practice meets all of the requirements of at least one of the sub-exceptions** in paragraphs **(b) through (e)** of this section.

(a) **Definitions** in this section.

(1) The term *HIPAA Privacy Rule* as used in this section means [45 CFR parts 160](#) and [164](#).

(2) The term *individual* as used in this section means one or more of the following—

(i) An individual as defined by [45 CFR 160.103](#).

(ii) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(iii) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section in making decisions related to health care as a personal representative, in accordance with [45 CFR 164.502\(g\)](#).

(iv) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(v) An executor, administrator, or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual’s estate under State or other law.

§ 171.202 Privacy Exception — When will an actor’s practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual’s privacy not be considered information blocking? (2)

(b) ***Sub-Exception – Precondition not satisfied.*** To qualify for the exception on the basis that **state or federal law requires one or more preconditions for providing access, exchange, or use of electronic health information have not been satisfied**, the following requirements must be met—

(1) The actor’s **practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either:**

(i) **Conforms to the actor’s organizational policies and procedures that:**

(A) **Are in writing;**

(B) **Specify the criteria to be used by the actor to determine when the precondition would be satisfied and, as applicable, the steps that the actor will take to satisfy the precondition; and**

(C) **Are implemented by the actor, including by providing training on the policies and procedures; or**

(ii) **Are documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met.**

§ 171.202 Privacy Exception — When will an actor’s practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual’s privacy not be considered information blocking? (2)

(2) **If the precondition relies on the provision of a consent or authorization** from an individual and the actor has received a version of such a **consent or authorization that does not satisfy all elements of the precondition required under applicable law**, the actor must:

(i) **Use reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or provide other reasonable assistance** to the individual to satisfy all required elements of the precondition; and

(ii) **Not improperly encourage or induce the individual to withhold the consent or authorization.**

(3) For purposes of determining whether the actor’s privacy policies and procedures and actions satisfy the requirements of subsections (b)(1)(i) and (b)(2) above **when the actor’s operations are subject to multiple laws which have inconsistent preconditions**, they shall be deemed to **satisfy the requirements of the subsections if the actor has adopted uniform privacy policies and procedures to address the more restrictive preconditions.**

§ 171.202 Privacy Exception — When will an actor’s practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual’s privacy not be considered information blocking? (3)

(c) **Sub-exception—health IT developer of certified health IT not covered by HIPAA.** If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, when engaging in a practice that promotes the privacy interests of an individual, the actor’s organizational privacy policies must have been disclosed to the individuals and entities that use the actor’s product or service before they agreed to use them, and must implement the practice according to a process described in the organizational privacy policies. The actor’s organizational privacy policies must:

- (1) **Comply with State and Federal laws**, as applicable;
- (2) Be **tailored to the specific privacy risk or interest being addressed**; and
- (3) Be **implemented in a consistent and non-discriminatory manner**.

Note: ONC states that “the vast majority of health IT developers of certified health IT operate as business associates to covered entities under HIPAA. As business associates, they are regulated by the HIPAA Privacy Rule” and would not need this sub-exception.

(d) **Sub-exception—denial of an individual’s request for their electronic health information** consistent with [45 CFR 164.524\(a\)\(1\) and \(2\)](#). If an individual requests electronic health information under the **right of access provision** under 45 CFR 164.524(a)(1) from an actor that must comply with 45 CFR 164.524(a)(1), the actor’s practice must be consistent with 45 CFR 164.524(a)(2).

§ 171.202 Privacy Exception — When will an actor’s practice of not fulfilling a request to access, exchange, or use electronic health information in order to protect an individual’s privacy not be considered information blocking? (4)

(e) ***Sub-exception—respecting an individual’s request not to share information.*** Unless otherwise required by law, an actor may elect not to provide access, exchange, or use of an individual’s electronic health information if the following requirements are met—

- (1) The individual requests that the actor not provide such access, exchange, or use of electronic health information without any improper encouragement or inducement of the request by the actor;
- (2) The actor documents the request within a reasonable time period;
- (3) The actor’s practice is implemented in a consistent and non-discriminatory manner; and
- (4) An actor may terminate an individual’s request for a restriction to not provide such access, exchange, or use of the individual’s electronic health information only if:
 - (i) The individual agrees to the termination in writing or requests the termination in writing;
 - (ii) The individual orally agrees to the termination and the oral agreement is documented by the actor; or
 - (iii) The actor informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual’s electronic health information except that such termination is:
 - (A) Not effective to the extent prohibited by applicable Federal or State law; and
 - (B) Only applicable to electronic health information created or received after the actor has so informed the individual of the termination.

§ 171.203 Security Exception—when will an actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information not be considered information blocking?

An actor’s practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information will **not be considered information blocking when the practice meets the conditions in paragraphs (a), (b), and (c) of this section**, and in addition **meets either the condition in paragraph (d) of this section or the condition in paragraph (e) of this section.**

- (a) The practice must be **directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.**
- (b) The practice must be **tailored to the specific security risk being addressed.**
- (c) The practice must be **implemented in a consistent and non-discriminatory manner.**
- (d) **If the practice implements an organizational security policy, the policy must—**
 - (1) **Be in writing;**
 - (2) Have been **prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the actor;**
 - (3) **Align with one or more applicable consensus-based standards or best practice guidance;** and
 - (4) **Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.**
- (e) **If the practice does not implement an organizational security policy, the actor must have made a determination in each case,** based on the particularized facts and circumstances, that:
 - (1) The **practice is necessary to mitigate the security risk to electronic health information;** and
 - (2) There are **no reasonable and appropriate 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 electronic health information. [Note: Revised in 11/4/2020 ONC Interim Final Rule with Comment]

§ 171.205 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 electronic health information not be considered information blocking? (1)

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 electronic health information **will not be considered information blocking** when the practice **meets a condition in paragraph (a), (b), (c), or (d)** of this section, as applicable to the particular practice and the reason for its implementation.

(a) *Maintenance and improvements to health IT.* When an actor implements a practice that makes health IT under that actor’s control **temporarily unavailable**, or **temporarily degrades the performance** of health IT, in order to perform maintenance or improvements to the health IT, the actor’s practice must be—

(1) Implemented for a period of time **no longer than necessary** to complete the maintenance or improvements for which the health IT was made unavailable or the health IT’s performance degraded;

(2) Implemented in a **consistent and non-discriminatory manner; and**

(3) **If the unavailability or degradation is initiated by a health IT developer of certified health IT, health information exchange, or health information network:**

(i) **Planned. Consistent with existing service level agreements** between the individual or entity to whom the health IT developer of certified health IT, health information exchange, or health information network supplied the health IT; or

(ii) **Unplanned. Consistent with existing service level agreements** between the individual or entity; **or agreed to by the individual or entity to whom** the health IT developer of certified health IT, health information exchange, or health information network **supplied the health IT.**

§ 171.205 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 electronic health information not be considered information blocking? (2)

(b) *Assured level of performance.* An actor may take **action against a third-party application that is negatively impacting the health IT’s performance**, provided that the practice is—

- (1) For a period of time **no longer than necessary** to resolve any negative impacts;
- (2) Implemented in a **consistent and non-discriminatory manner**; and
- (3) **Consistent with existing service level agreements**, where applicable.

(c) *Practices that prevent harm.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a **risk of harm** to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception. **[Harm Exception]**

(d) *Security-related practices.* If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception. **[Security Exception]**