The Office of the National Coordinator for Health Information Technology

What Clinicians and Other Health Care Providers Need to Know

How the Exceptions Support Providers, Patients, and Information Sharing: Part 3

February 2, 2022

General Disclaimers

- **The information in this presentation is based on the regulations in 45 CFR Part 171.**
- While every effort has been made to ensure accuracy, this presentation is not a legal document. Please note that other federal, state and local laws may apply.
- Examples are merely illustrative and may be simplified for ease of discussion.
- Any practice (act or omission) that implicates the information blocking regulations may come under investigation by HHS.
- This communication is produced and disseminated at U.S. taxpayer expense.

Speakers

LaVerne M. Perlie, MSN, BSN, RN
Nurse Consultant, Office of Policy
HHS/ONC

Cassie Weaver, JD
Policy Analyst, Office of Policy
HHS/ONC

Grace Castro, JD, MPH
Policy Analyst, Office of Policy
HHS/ONC

ONC Clinical Council

- Thomas Mason, MD Chief Medical Officer
- Kiri Bagley, MD
- Wanda Govan-Jenkins, DNP, MS, MBA, RN
- David R. Hunt, MD, FACS
- Thomas Keane, MD
- Elizabeth Palena-Hall, MIS, MBA, RN
- LaVerne M. Perlie, MSN, BSN, RN
- Tricia Lee Rolle, PharmD
- Albert Taylor, MD

Learning Objectives

- Review 4 Exceptions to Information Blocking
  - Health IT Performance Exception
  - Preventing Harm Exception
  - Privacy Exception
  - Security Exception
- Identify where to find more information and educational resources

Eight Information Blocking Exceptions

- **Information Sharing**: the norm is to avoid actions or omissions ("practices") that are likely to interfere with information sharing.
- **Exceptions**: the exceptions offer assurance that **reasonable and necessary** "practices" covered by an exception will **not** be **considered information blocking**.

Applicable to delaying, restricting, or denying access, exchange, or use	Applicable to processes or procedures for fulfilling access, exchange, or use of EHI
1. Infeasibility Exception	6. Content and Manner Exception
2. Preventing Harm Exception	7. Fees Exception
3. Privacy Exception	8. Licensing Exception
4. Security Exception	
5. Health IT Performance Exception	

Setting the Stage for Some Real-World Examples

- Examples we discuss today are illustrative examples and are not a comprehensive catalog. Many other types of actions or omissions ("practices") could also implicate the information blocking provision.
- A determination as to whether a "practice" would be information blocking requires a fact-based, case-by-case assessment.
- Such a case-by-case assessment considers all relevant individual facts and circumstances against ***all*** the elements of information blocking.
- For ease of discussion, samples focus on the likelihood of a "practice" being an "interference," but practices likely to interfere are "information blocking" only if they meet ***all*** elements of information blocking.

Elements of Information Blocking

- Not "required by law"
- Not covered by an exception
- Likely to "interfere with" access, exchange, or use
- Electronic health information (EHI)
- By an "Actor"
- Requisite knowledge of "Actor"

Who is covered by the information blocking regulations?

Health IT Developers of Certified Health IT | Health Information Networks & Health Information Exchanges | Health Care Providers

Information Blocking Exceptions

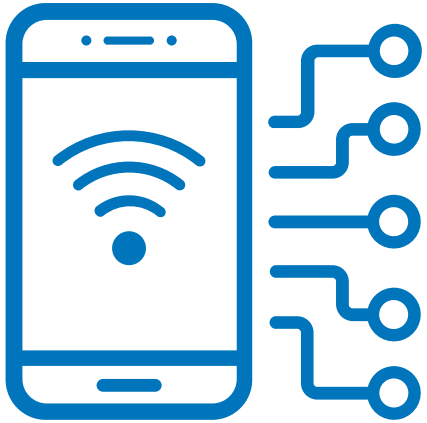
Satisfying the conditions and documenting use of an exception:

- Failure to meet an exception does not mean that an actor's practice meets the information blocking definition.
- The actor's documented records should reflect what would be needed to demonstrate the actor met each of the conditions or requirements of the exception.
  - Actors have substantial flexibility to determine where to document specific types and pieces of information — in the EHR or elsewhere in their overall records.

Health IT Performance Exception

Overview

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



To qualify for this exception, an actor's practice must meet one of the following conditions:

Maintenance and improvements to health IT

OR

Assured level of performance

OR

Practices that prevent harm

OR

Security-related practices

Using the Health IT Performance Exception

Question:

- If I am experiencing a significant negative impact on the performance of my health IT because of the behavior of a third-party application, can I use throttling on certain health IT functions to maintain the performance of my health IT without being considered an information blocker?

Health IT Performance Exception:

To qualify for this exception, an actor's practice must meet one of the following conditions:

1. Maintenance and improvements to health IT; OR
2. Assured level of performance; OR
3. Practices that prevent harm; OR
4. Security-related practices.

*"Practices" will be evaluated on a case-by-case basis to determine whether information blocking has occurred. A practice likely to be an interference may not be information blocking if the actor's practice is required by law, satisfies the conditions of an exception, or is done without the knowledge required on the part of the actor by the information blocking definition.

Preventing Harm Exception

Overview

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

To satisfy this exception:

The actor must hold a reasonable belief that the practice will substantially reduce a risk of harm *and* the practice must be no broader than necessary

+

The practice must satisfy at least one condition from each category: type of risk, type of harm, *and* implementation basis

+

The practice must satisfy the condition concerning a patient right to request review of an individualized determination of risk of harm

Using the Preventing Harm Exception

Question:

- My ICU patient dies while their spouse was not able to be in the hospital with them. In my professional judgment, it is reasonably likely that patient's spouse will suffer substantial psychological or emotional harm from first learning via a portal or app that their spouse has died. Can the Preventing Harm Exception cover delaying availability of patient death information in the portal or API until I or a fellow clinician can break the news to them in real time?

Preventing Harm Exception:

- Where *type of risk* is **individually determined**, the actor must meet six conditions:
  - *Reasonable belief*;
  - *Practice breadth;*
  - *Type of risk;*
  - *Type of Harm;*
  - *Practice implemented based on an organizational policy or a determination specific to the facts and circumstances;*

  &
  - *Patient right to request review of individualized determination of risk of harm.*

*"Practices" will be evaluated on a case-by-case basis to determine whether information blocking has occurred. A practice likely to be an interference may not be information blocking if the actor's practice is required by law, satisfies the conditions of an exception, or is done without the knowledge required on the part of the actor by the information blocking definition.

Additional Resources:

- ONC's Information Blocking FAQs on HealthIT.gov

Privacy Exception

Overview

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

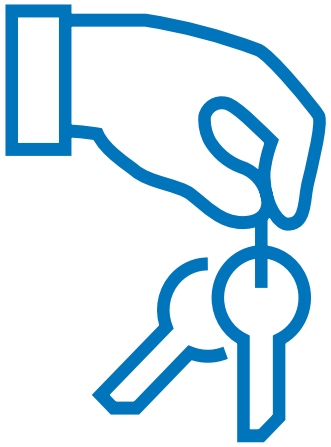
To satisfy this exception, an actor's privacy-protective practice must:

Satisfy at least one of the following 4 sub-exceptions

- **Pre-condition not satisfied**
- **Health IT developer of certified health IT not covered by HIPAA**
- **Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a)(1) and (2)**
- **Respecting an individual's request not to share information**

+

Meet all conditions applicable to a sub-exception being relied upon



Privacy Exception: The Four Sub-exceptions

- An actor's practice of not fulfilling a request to access, exchange, or use EHI 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 this section.

(b) precondition not satisfied

(c) health IT developer of certified health IT not covered by HIPAA

(d) denial of an individual's request for their EHI consistent with 45 CFR 164.524(a)(1) and (2)

(e) respecting an individual's request not to share information

Using the Privacy Exception

Questions:

- As a provider, a patient requested that I disclose their EHI regarding a sensitive health condition. My state requires an individual's consent to disclose such information. The consent that the patient provided did not satisfy all of the legal requirements for disclosure. Can I use the "precondition not satisfied" sub-exception to deny the request?

- As a provider, my patient has explicitly asked me to NOT share their SDOH data with anyone but did not elaborate on their reasoning for wanting to keep that information confidential. My state does not require me to get specific consent to disclose SDOH data to my patient's other healthcare providers. Can I use the privacy exception in this instance to NOT share my patient's SDOH data?

Privacy Exception:

An actor's practice of not fulfilling a request to access, exchange, or use EHI in order to protect an individual's privacy will not be considered information blocking when the practice(s) meets ***all*** of the requirements of ***at least one*** of the 4 available sub-exceptions:

1. Pre-condition not satisfied
2. Health IT developer of certified health IT not covered by HIPAA
3. Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a)(1) and (2)
4. Respecting an individual's request not to share information

*"Practices" will be evaluated on a case-by-case basis to determine whether information blocking has occurred. A practice likely to be an interference may not be information blocking if the actor's practice is required by law, satisfies the conditions of an exception, or is done without the knowledge required on the part of the actor by the information blocking definition.

Security Exception

Overview

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

To satisfy this exception, an actor's security-related practice must:

Be directly related to safeguarding the confidentiality, integrity, and availability of EHI

+

Be tailored to specific security risks; and

+

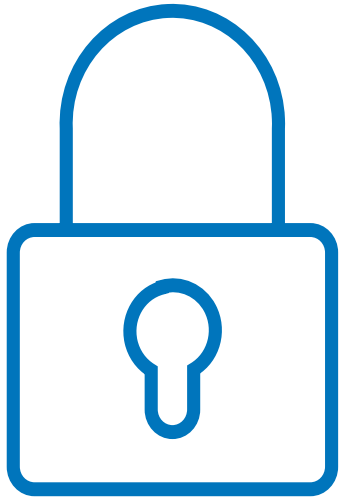
Be implemented in a consistent and non-discriminatory manner; and

+

Implement a qualifying organizational security policy

OR

Implement a qualifying security determination



Using the Security Exception

Questions:

- I am a hospital with a very robust data security program. I have specific concerns about the data security of a physician practice in my area. Will the Security Exception cover my denying that doctor access to EHI of patients we both treat in order to better protect the EHI from a potential breach?

- My patient wants me to release their EHI to a third-party app they have chosen. I am satisfied I can release the EHI without compromising my systems or legal obligations under HIPAA. But my reputation will suffer if I let patients send their EHI to an app that then gets breached. Will the Security Exception cover my refusing to release the patient's EHI as long as I do the same for every app I haven't assessed for security or if I am not satisfied with how the app handles EHI once it's in the app?

Security Exception:

To satisfy this exception, an actor's security-related practice must:

1. Be directly related to safeguarding the confidentiality, integrity, and availability of EHI
2. Be tailored to specific security risks; and
3. Be implemented in a consistent and non-discriminatory manner; and
4. Either
   - A. Implement a qualifying organizational security policy; OR
   - B. Implement a qualifying security determination

*"Practices" will be evaluated on a case-by-case basis to determine whether information blocking has occurred. A practice likely to be an interference may not be information blocking if the actor's practice is required by law, satisfies the conditions of an exception, or is done without the knowledge required on the part of the actor by the information blocking definition.

Where To Find More Information

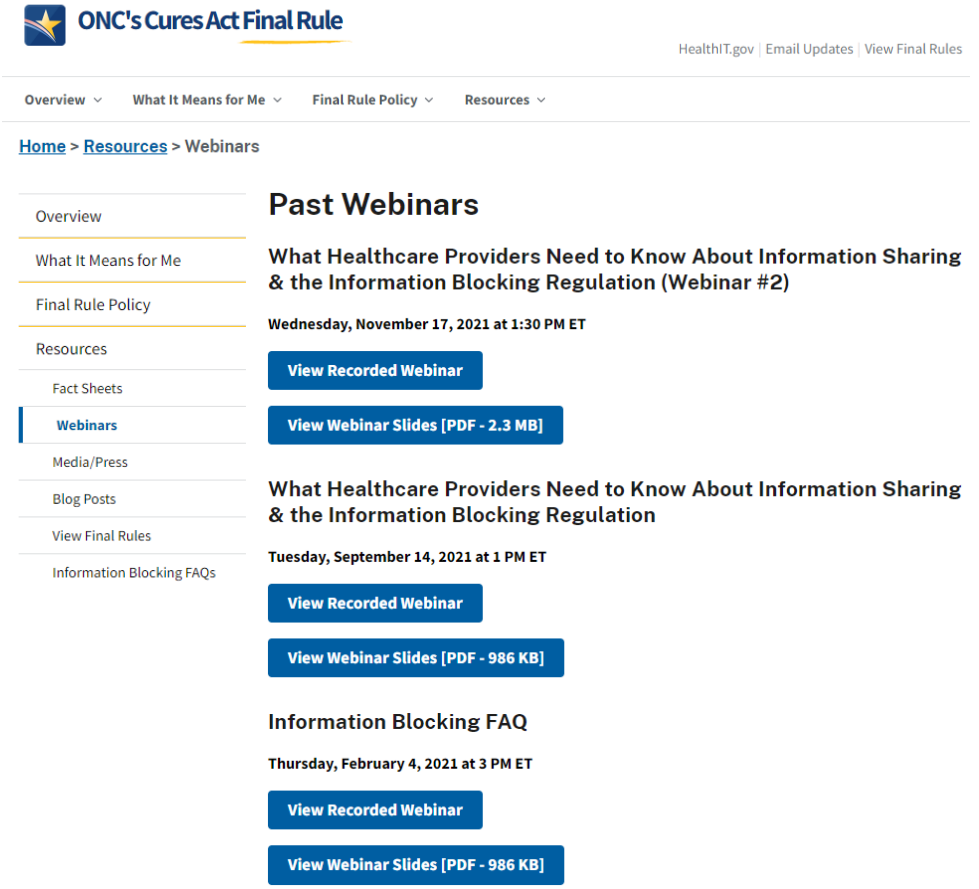
- **ONC Website Resources:** www.HealthIT.gov/CuresRule

Factsheets: https://www.healthit.gov/curesrule/resources/fact-sheets

FAQs: https://www.healthit.gov/curesrule/resources/information-blocking-faqs

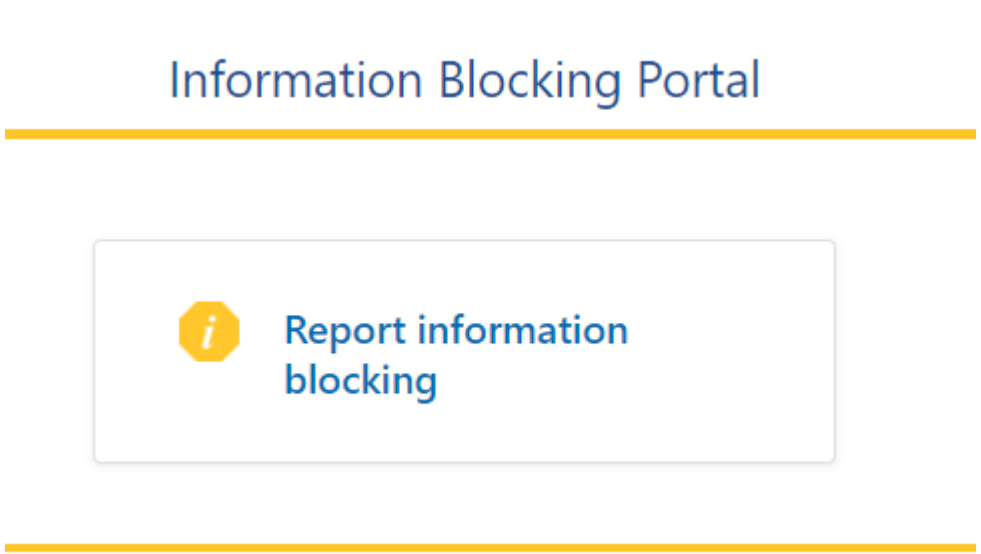
Blogs: https://www.healthit.gov/buzz-blog/category/21st-century-cures-act

Webinars: https://www.healthit.gov/curesrule/resources/webinars



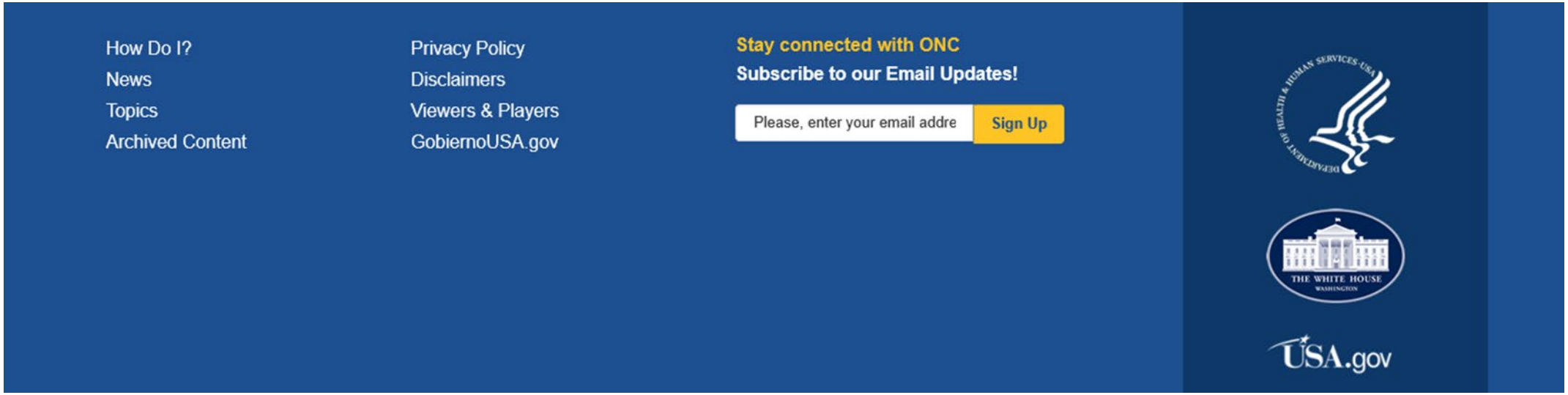
What if You Are Experiencing Information Blocking?

- The Cures Act directs the National Coordinator to implement a standardized process for the public to submit claims of potential information blocking.
- A report of potential information blocking can be submitted through the Report Information Blocking Portal: https://healthit.gov/report-info-blocking



Upcoming Events

- ***"Ask ONC About Information Sharing" on* February 3, 2022**
- ***ONC Annual Meeting on* April 13-14, 2022**
- For information on upcoming webinars and events, subscribe to ONC email updates at **www.healthit.gov**



The Office of the National Coordinator for Health Information Technology

Contact ONC

Health IT Feedback Form:
https://www.healthit.gov/form/healthit-feedback-form

Twitter: @onc_healthIT

LinkedIn: Search “Office of the National Coordinator for Health Information Technology”

HealthIT.gov

Subscribe to our weekly eblast at healthit.gov for the latest updates!