The Office of the National Coordinator for Health Information Technology

21ST CENTURY CURES ACT:
INTEROPERABILITY, INFORMATION BLOCKING, AND
THE ONC HEALTH IT CERTIFICATION PROGRAM PROPOSED RULE

Information Blocking Exception for Privacy-Protective Practices

OVERVIEW

Under the proposed exception, it will not be information blocking for an actor to engage in certain recognized privacy-protective practices that interfere with the access, exchange, or use of electronic health information (EHI), and that are reasonable and necessary.

The proposed exception is structured under four discrete sub-exceptions that have been crafted to closely mirror privacy-protective practices that are recognized under state and federal privacy laws.

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

Satisfy at least one sub-exception

+

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

Objective

If an actor is authorized to provide access, exchange, or use of EHI under a privacy law, then the information blocking provision would require that the actor provide that access, exchange, or use of EHI.

However, the information blocking provision should not require the use or disclosure of EHI in a way that is prohibited under state or federal privacy laws.

This proposed exception would operate in a manner consistent with the framework of the HIPAA Privacy Rule and uphold privacy rights that patients now have.

"Actors" regulated by the information blocking provision:

- Health Care Providers
- Health IT Developers of Certified Health IT
- Health Information Exchanges
- Health Information Networks

Sub-exception | Precondition not satisfied

If an actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of EHI, the actor may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied. Certain conditions must be met:

The practice must implement and conform to the actor's written organizational policies and procedures that specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition be satisfied and the practice will be consistently applied.

or

The practice is 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.

- The practice must be tailored to the specific privacy risk or interest being addressed;
- The practice must be implemented in a consistent and non-discriminatory manner; and
- If the precondition relies on the provision of consent or authorization from a person, the actor:
  - Did all things reasonably necessary within its control to provide the person with a meaningful opportunity to provide the consent or authorization; and
  - Did not improperly encourage or induce the person to not provide the consent or authorization.

Example preconditions—

- A privacy law that requires that a person provide consent before her EHI can be accessed, exchanged, or used for specific purposes.
- A privacy law that authorizes the disclosure of EHI only once the identity and authority of the person requesting the information has been verified.

Applying the conditions

The HIPAA Privacy Rule generally requires covered entities (and their business associates) to take reasonable steps to limit the use or disclosure of protected health information to the minimum necessary to accomplish the intended purpose. An actor could meet the requirements of this sub-exception while exchanging less EHI than requested by another entity. The actor would not be information blocking if it implemented a written minimum necessary organizational policy and procedure in a manner tailored to the risk of disclosing more than the minimum necessary, and did so in a non-discriminatory and consistent manner.

Sub-exception | Health IT developer of certified health IT not covered by HIPAA

If an actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, the actor may choose to interfere with access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are met.

We expect the class of health IT developer of certified health IT that utilizes this exception to be very small. The overwhelming majority of health IT developers of certified health IT are regulated by the HIPAA Privacy Rule as business associates.

The practice must:

- Comply with applicable state or federal privacy laws;
- Implement a process that is described in the actor's organizational privacy policy;
- Have previously been meaningfully disclosed to the persons and entities that use the actor's product or service;
- Be tailored to the specific privacy risk or interest being addressed; and
- Be implemented in a consistent and non-discriminatory manner.

Sub-exception | Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3)

An actor that is a covered entity or business associate may deny an individual's request for access to their protected health information in the circumstances provided under 45 CFR 164.524(a)(1), (2), and (3) of the HIPAA Privacy Rule.

There are no information blocking conditions to be met for this exception. However, conditions prescribed under each of 45 CFR 164.524(a)(1), (2), and (3) would need to be met, as applicable.

45 CFR 164.524(a)(1), (2), and (3) deals with:

- Certain requests made by inmates of correctional institutions
- Information created or obtained during research that includes treatment, if certain conditions are met
- Denials permitted by the Privacy Act
- Information obtained from non-health care providers pursuant to promises of confidentiality
- Psychotherapy notes
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
- Additional reviewable and unreviewable grounds by licensed health care providers

Sub-exception | Respecting an individual's request not to share information

In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual. Certain conditions must be met:

- The individual must have requested that his or her EHI not be accessed, exchanged, or used;
- The request must have been initiated by the individual without any improper encouragement or inducement by the actor;
- The actor or its agent must have documented the request within a reasonable time period; and
- The practice must be implemented in a consistent and non-discriminatory manner.

- An actor may give effect to an individual's request even if state or federal laws would allow the actor to ignore the individual's request.
- This sub-exception would not operate to permit an actor to refuse to provide access, exchange, or use of EHI when that access, exchange, or use is required by law.