COSMOS
Navigate the Compliance Universe

Compliance Today - January 2023

Dawn Morgenstern (dawn.morgenstern@clearwatercompliance.com, linkedin.com/in/dawn-morgenstern/) is Director, Consulting Services at Clearwater Compliance LLC, Nashville, TN.

Understanding information blocking and the expectations for healthcare organizations

by Dawn Morgenstern, MBA, CHPC, CCSFP

In April 2021, the 21st Century Cures Act Final Rule went into effect, prohibiting healthcare entities from information blocking to break down barriers that have historically limited patient access to electronic personal health information (ePHI). To allow entities an opportunity to phase in their compliance, the initial rollout of the rule only covered a subset of electronic health information (EHI). However, as of October 6, 2022, entities will be responsible for complying with information blocking as it applies to the full scope of EHI.

Information blocking may be the most important change to health information since HIPAA. However, it's important to point out that information blocking is not a HIPAA rule and applies to all healthcare providers—not just HIPAA-covered entities.

Information blocking relates to any practice that might interfere with access, exchange, or use of ePHI, including any designated record set, regardless if a covered entity maintains the group of records or if the records are maintained for a covered entity.

In short, with few exceptions, healthcare providers, tech vendors, health information exchanges, and health information networks (HIN) can't prevent EHI access. The rule assumes that if HIPAA permits a patient or any other entity or individual to access records, they should be given access without delay, using almost any technology the requester chooses. Those requests do not have to be event-triggered.

For healthcare providers, it's about knowing which practices are considered unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

If an organization fails to provide access, without delay, to a person permitted access under HIPAA and other laws, that may be considered information blocking.

The ultimate goal is to improve healthcare data flow and facilitate improved and coordinated patient care with more patient engagement in healthcare decisions.

Who must be compliant?

Information blocking affects three types of entities:

1. Healthcare providers (regardless of HIPAA status).
2. Health information exchanges (HIE) and HIN. This is broadly defined and can include any entity that helps

two or more providers exchange data. It also applies to a HIPAA business associate if the associate has an exchange role.

3. Health IT developers who offer Certified Electronic Health Record Technology.

If any of these organizations are also HIPAA-covered entities, there is an expectation that they must comply with HIPAA and the rules of the 21st Century Cures Act. Healthcare providers who aren't HIPAA-covered entities must still comply with information blocking.

Exceptions to information blocking

There are two categories of exceptions applicable to information blocking: denial exceptions, and approval and process exceptions related to how requests are fulfilled.

There are eight specific exceptions, with complex implementation standards that allow providers to deny ePHI requests without being seen as information blocking. The following is an overview of those exceptions.

Denial exceptions

1. Preventing harm exception

The preventing harm exception recognizes that organizations may deny requests if doing so protects patients or others from harm. Therefore, it's essential to document the potential risk and harm that triggered the exception.

In using this exemption, healthcare providers must demonstrate:

- A reasonable belief that access denial would substantially reduce the risk of harm to a patient or another person that would otherwise occur if fulfilled.
- Denial must be no broader than necessary to substantially reduce the risk of harm.
- There are two ways to determine risk of harm. The first is on an individualized basis when a licensed healthcare professional (who has a current or prior clinician–patient relationship with the patient) is exercising professional judgment. The other way is from data known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.[1]

2. Privacy exception

The privacy exception recognizes that an organization should not be required to use or disclose ePHI in a way that state or federal privacy laws prohibit. Information blocking does not render those laws obsolete.

"To satisfy this exception, [an organization's] privacy-protective practice must meet at least one of the four sub-exceptions:

- "***Precondition not satisfied***: If [an organization] is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing access, exchange, or use of EHI, [it] may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances.
- "***Health IT developer of certified health IT not covered by HIPAA:*** If an [organization] is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, [it] may choose to interfere with the access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are

met.

- "***Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a) (1) and (2):*** An [organization] that is a covered entity or business associate may deny an individual's request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.
- "***Respecting an individual's request not to share information:*** An [organization] may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided certain conditions are met."[2]

This exception mirrors HIPAA Privacy Rule provisions about which ePHI patients can access.

It's worth noting that it could be considered information blocking if an organization encourages patients to allow their providers access but infer the patient should be more selective in agreeing to access for others.

3. Security exception

The security exception covers all legitimate security practices by organizations but does not prescribe a maximum level of security or dictate a one-size-fits-all approach.

It is not considered information blocking if an organization interferes with access to protect ePHI security.

For instance, a practice believes data release would compromise data security. If a request threatens patient information, the security exception may be applicable. This should be consistent, nondiscriminatory, and tailored to specific security threats. It doesn't cover practices that claim to promote security but are unreasonably broad and onerous. The security exception should not be a broad brush for request denials.

If an organization uses this exception, it must demonstrate that the denial is directly related to ePHI safeguarding based on specific security risks. That should include updated and relevant privacy and security policies. If those don't exist, the organization should implement those to help mitigate practices that could prohibit or delay ePHI data sharing.

4. Infeasibility exception

The infeasibility exception notes that legitimate challenges could limit an organization's ability to comply with a request. For example, the organization may not have—and may be unable to get—requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use.

An organization may deny a request if it is considered infeasible. Before applying this exception, see if other exceptions may be more appropriate. The infeasibility exception should cover issues outside of an organization's control.

The practice must meet one of the following conditions:

- "Uncontrollable events: [The organization] cannot fulfill the request for access, exchange, or use of [EHI] due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
- "Segmentation: [The organization] cannot fulfill the request for access, exchange, or use of [EHI] because [it] cannot unambiguously segment the requested [EHI].

- "Infeasibility under the circumstances: [The organization] demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances."[3]

If using this exception, the organization should provide a written response to the requester within 10 business days of getting the request, including why the request is infeasible.

5. Health IT performance exception

The health IT performance exception recognizes that it requires maintenance and sometimes improvements for health IT to perform properly and efficiently. This may require some health IT systems to go offline temporarily and can be for scheduled or unscheduled reasons.

The practice must:

1. "Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
2. "Be implemented in a consistent and non-discriminatory manner; and
3. "Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN."[4]

An organization may act against a third-party app 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.

"If the unavailability is in response to a risk of harm or security risk, [the organization] must only comply with the Preventing Harm or Security Exception, as applicable."[5]

The IT performance exception is for those issues that temporarily prohibit access and should be used consistently and in a nondiscriminatory manner.