**Information Blocking Exceptions and Use Cases**

*Please note: This document has been created to educate providers and other clinical staff about the 6 of the 9 most applicable exceptions to information blocking. This document does not constitute legal advice. To make sure your health center complies with the Cures Act and HTI-1 rules when using an exception, please discuss it with your health center’s legal counsel.*

For each of those exceptions all of the applicable criteria must be met and documented. In addition, it is generally understood that these exceptions will be uniformly and consistently applied.

**Preventing Harm Exception:** If sharing certain electronic health information (EHI) with the patient, the patient’s legal representative, or other authorized requestor is reasonably likely to cause harm to the patient or another person, a health care provider may restrict access to that information to prevent harm if all the required conditions of this exception are met:

* + The actor must hold a reasonable belief that the practice will substantially reduce a risk of harm;
	+ The actor’s practice must be no broader than necessary;
	+ The actor’s practice must satisfy at least one condition from each of the following categories: type of risk, type of harm, and implementation basis; and
	+ The practice must satisfy the condition concerning a patient’s right to request a review of an individualized determination of the risk of harm.
	+ **Scenario 1:** A patient comes in for an encounter with her mental health counselor. The counselor notes in the record that the patient’s appearance is disheveled and thoughts are disorganized; such that the counselor has concerns of schizophrenia. The patient has previously expressed that if she cannot understand reality, she would rather die. The patient has established a patient portal where she can review provider notes. The counselor is seriously concerned that if the patient reads the treatment notes, she will become immediately suicidal.

 **What to do:** Under the Information Blocking Rules, the counselor can restrict certain EHI from going into the portal if the counselor believes that the patient is in imminent danger of harming herself, but under HIPAA and New York law, the patient needs to be informed in written communication that certain information has been withheld from the portal and that she has an opportunity to appeal.

* + **Scenario 2**: A patient in his mid-twenties is frequently seen by his provider because of migraines. He expresses that he thinks his migraines are the result of his mother’s constant criticism of him and her general intrusion into his life. As an adult, the mother would not have the right to access the records. However, when the patient dies in a car accident, the mother is entitled to the records. The provider also treats the mother and has significant concern for her physical, emotional and psychological well-being if she sees the comments made by her deceased son.

**What to do**: If the mother requests copies of the records, the provider can redact the notes that he fears would cause the mother harm; however under HIPAA and New York law, the mother needs to be informed in a written communication that certain information has been redacted and that she has an opportunity to appeal.

* + **Scenario** **3**: The oncological physician staff requests that oncology test results not be put into the patient portal until the physician has reviewed them and contacted the applicable patient, which can be a week to 10 days.

**What to do**: The Information Blocking guidance indicates that this type of generalized concern of harm does not meet the Preventing Harm Exception, and lab tests should be included in the portal as soon as received.

1. **Privacy Exception:** If disclosing certain EHI would violate federal or state privacy laws, such as HIPAA, providers may restrict access to protect patient privacy. There are four sub-exceptions:

**Precondition Not Satisfied -** A health care provider may choose not to provide access, exchange or use of EHI protected by a state or federal law that requires certain conditions, such as completion of a consent or authorization form.

**Respecting a patient’s request not to share information-** A health care provider may choose not to provide access, exchange or use of EHI if the patient requests that the health care provider not access, exchange, or use their EHI.

**Health IT developer of certified health IT not covered by HIPAA -** If a health care provider is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, the health care provider 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) -** A health care provider 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.

* + **Scenario 1:** A patient comes to the health center for follow-up treatment following a D&C. The patient asks that her health plan not be billed or informed of the treatment and that agrees to pay for all related treatment out-of-pocket.

**What to do:** The Center is not permitted to provide the information to the insurance plan and cannot respond to inquiries from the health plan about such treatment.

* + **Scenario 2**: The Center receives a subpoena for medical records of a patient involved in a personal injury suit. The subpoena is not accompanied by a patient authorization or court order, one of which is necessary in order to comply with HIPAA and overcome the NY physician-patient privilege.

**What to do**: The Center can require the person issuing a subpoena to provide a patient authorization or court order before the information is released.

1. **Security Exception:** Denial of access to EHI for security reasons will not be considered information blocking if the denial is directly related, and tailored, to safeguarding the confidentiality, integrity, and availability of EHI and meets one of the following:
* Is based upon a written security policy prepared on the basis of security risk analysis and provides objective timeframes for addressing security incidents.
* A determination has been made that the practice is necessary to mitigate an EHI security risk and there are no reasonable and appropriate alternatives.
	+ **Scenario:** A health care organization identifies a critical security vulnerability in its electronic health record system. The organization’s security policy requires the Security Officer to shut down access to the network when a security vulnerability is identified.

**What to do:** To prevent a data breach, the organization can temporarily restrict access to the system until the security vulnerability is addressed and the system is secure.

1. **Infeasibility Exception:** If it is technically or organizationally infeasible for a healthcare provider to share specific EHI due to limitations in their systems or infrastructure, they may qualify for this exception. The practice must meet one of the following conditions:

**Uncontrollable events**- The health care provider cannot fulfill the request for access, exchange, or use of electronic health information 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 health care provider cannot fulfill the request for access, exchange, or use of EHI because the health care provider cannot unambiguously segment the requested EHI.

**Infeasibility under the circumstances**- The health care provider 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.

*The health care provider must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.*

* + **Scenario:** The Center does not wish to include in the patient portal for adolescents information about pregnancy, abortion, or sexually transmitted disease treatment because of concern that a parent who also has access to the portal might see such information. The portal software is unable to segregate such information.

**What to do:** The Center decides that, because it is infeasible to segment such information, it will not offer a patient portal to adolescents. Instead adolescents can request a copy of their records from HIM (which can review the records and remove any specially protected information). In order to address the notification requirements, the Center places a notice on the patient portal sign on page, that adolescents need to contact the HIM department for access to medical records because of the infeasibility of maintaining a patient portal for adolescents. Note: *the ONC has not commented on this strategy so it is not yet known if it will comply but many providers have adopted this strategy rather than allowing for inappropriate disclosure to parents.*

1. **Health IT Performance Exception:** This exception applies when the health care provider’s health IT is temporarily unavailable, or the performance of health IT is temporarily degraded, in order to perform maintenance or improvements to the health IT. During this time, the healthcare provider is unable to fulfill request for access and exchange of EHI because of planned and unplanned system. This exception can only 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; and be implemented in a consistent and non-discriminatory manner.
	* **Scenario:** A healthcare provider has recently implemented a new electronic health record (EHR) system and unexpected technical issues arise that impact the system's performance.
	* **What to do:** To prevent widespread disruptions, the provider may temporarily restrict access to EHI until the technical issues are resolved and the system is functioning optimally.
2. **Manner Exception:** Healthcare providers are expected to make reasonable attempts to disclose requested information in the format/manner requested. If the health care provider cannot do so, the request should be fulfilled in an alternative manner that uses one of the following, in the given order of priority:
	* + Certified health IT, such as a certified EHR;
		+ Content and transport standards published by the Federal government;
		+ Content and transport standards of an organization accredited by ANSI (American National Standards Institute); or
		+ An alternative machine-readable format (XML, CSV or other structured data format).

NOTE: If it remains infeasible to fulfill the request using the methods listed above, or agreement with the requestor cannot be reached for providing the requested information using an alternative manner, then the Entity may invoke the Infeasibility Exception (see above). In such an event, the individual processing the request will prepare a written response explaining why the request is infeasible. The response will be provided to the requestor within ten (10) business days of the original request.

* + **Scenario:** The Center receives a request from a patient to send the patient a portion of his medical record via encrypted email. The Center does not have the technical capability to send encrypted email from its EHR and offers to send the requested information on an encrypted zip drive or CD or that the patient may obtain the patient portal. The patient refuses.
	+ **What to do:** The Center should send a letter to the patient pursuant to the infeasibility exception.