Information Blocking: Exceptions Policy

Policy

{{OrgName}} has implemented policies to prevent practices which restrict access, exchange, or use of Electronic Health Information for treatment and other permitted purposes.

{{OrgName}}'s policies to prevent information blocking take into account exceptions permitted under the CURES Act, Information Blocking Rule.

If it is deemed necessary to withhold the information under any of the below exceptions, {{OrgName}} will document the harm assessment and retain the documentation for no less than 6 years.

Preventing Harm Exception

{{OrgName}} may deny a request to access, exchange, or use Electronic Health Information if there is a reasonable belief that withholding the information will reduce a risk of harm. {{OrgName}} will not restrict data beyond what is necessary to prevent harm.

To enact this exception, the restriction must satisfy one condition form each of the following categories:

- Type of risk
- Type of harm
- Implementation basis

The patient has the right to review the individualized determination of risk of harm.

Privacy Exception

{{OrgName}} may deny a request to access, exchange, or use Electronic Health Information to protect individual privacy if:

- Precondition not satisfied:
  - {{OrgName}} may deny a request if there is a federal or state regulation which requires a precondition, such as patient consent/authorization. This exception does not include {{OrgName}} policies which are stricter than a regulation/law.
- Request is not permitted under the HIPAA Privacy Rule:
  - {{OrgName}} may deny a request for access to PHI under the circumstances provided under 45 CFR 164.524(a)(1)and(2).
    - Psychotherapy Notes
  - {{OrgName}} recognizes that access, exchange, or use of PHI is permissible under the Treatment, Payment, and Operations provision of the HIPAA Privacy

Rule and will not block information nor implement barriers to access for this type of data exchange/access.

- Respecting an individual’s request not to share: {{OrgName}} may choose not to provide access, exchange, or use of an individual’s Electronic Health Information if doing so fulfills the wishes of the individual, provided certain conditions are met.

Security Exception

{{OrgName}} may deny a request to access, exchange, or use Electronic Health Information to protect the security of the data. This exception is meant to cover all legitimate security protocols and practices.

- The denial must be directly related to safeguarding the confidentiality, integrity, and availability of the Electronic Health Information.
- Must be tailored to specific security risks
- Must be implemented in a consistent and non-discriminatory manner
- Must implement a security policy or qualifying security determination

Infeasibility Exception

{{OrgName}} shall invoke the infeasibility exception to the Information Blocking Rule, when legitimate practical challenges limit {{OrgName}} from complying with a request to access, exchange, or use Electronic Health Information. Legitimate practical challenges exist when {{OrgName}} does not have and/or is unable to obtain the technological capabilities, legal rights, or other means necessary to enable the request.

Uncontrollable events such as: 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 disruption, or act of military, civil, or regulatory authority, make complying with the request infeasible.

Electronic Health Information cannot be unambiguously segmented.

{{OrgName}} 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.

{{OrgName}} must provide written notice to the requestor within 10 days of the receipt of the request with the reason as to why the request is infeasible.

Health IT Performance Exception

{{OrgName}} takes 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. This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that health IT be taken offline temporarily.

- The practice must:
    - 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;
    - Be implemented in a consistent and non-discriminatory manner; and
    - Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN.
- {{OrgName}} may take action against a third-party app that is negatively impacting the health IT's performance, provided that the practice is:
    - For a period of time no longer than necessary to resolve any negative impacts;
    - Implemented in a consistent and non-discriminatory manner; and
    - Consistent with existing service level agreements, where applicable.
- If the unavailability is in response to a risk of harm or security risk, the clinic or hospital must only comply with the Preventing Harm or Security Exception, as applicable.

Content and Manner Exception

This exception provides {{OrgName}} flexibility concerning content and manner of a response to a request.

Content Condition

For 24 months from the publication date (March 9, 2020) of the CURES Act, {{OrgName}} must respond to requests for access, exchange, or use of Electronic Health Information identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard:

- Allergies and Intolerances
- Goals
- Problems
- Assessment and Plan of Treatment
- Health Concerns
- Procedures
- Care Team Members
- Immunizations
- Provenance
- Clinic Notes
- Laboratory
- Smoking Status
- Medications
- Unique Device Identifiers
- Diagnostic Imaging
- Patient Demographics
- Vital Signs
- Encounter Information

After March 9, 2022, {{OrgName}}, must respond to requests for access, exchange, or use of Electronic Health Information identified by the data elements as defined in §171.102 of the CURES Act:

- Patient Name
- Sex (as defined in §170.207(n)(1)
    - Birth Sex attributed as follows
        - Male
        - Female
        - Unknown
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Smoking Status
- Problems
- Medications
- Medication allergies
- Laboratory tests
- Laboratory value/results
- Vital signs
- Procedures
- Care team members
- Immunizations
- Unique device identifiers
- Assessment and plan of treatment
- Goals
- Health concerns

Manner Condition
{{OrgName}} may need to fulfill a request in an **alternative manner** when we are:

- Technically unable to fulfill the request in any manner requested; ***or***
- Cannot reach agreeable terms with the requestor to fulfill the request.

If {{OrgName}} fulfills a request in an alternative manner, such fulfillment must comply with the order of priority described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

Fee Exception

{{OrgName}} may charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using Electronic Health Information, provided certain conditions are met. This exception enables {{OrgName}} to charge fees related to the development of technologies and provision of services that enhance interoperability.

Fees must:

- Be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests.
- Be reasonably related to the {{OrgName}}'s costs of providing the type of access, exchange, or use of EHI.
- Not be based on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor.

Licensing Exception

{{OrgName}} is permitted to protect its innovations and to charge reasonable royalties in order to earn returns on the investments we have made to develop, maintain, and update our innovations to support interoperability elements for Electronic Health Information to be accessed, exchanged, or used.

Licensing negotiations must begin within 10 business days of receipt of a request and negotiate a licensing fee within 30 days from receipt of the request.

Licensing conditions must include:

- Scope of rights
- Reasonable royalty
- Non-discriminatory terms
- Collateral terms
- Non-disclosure agreement

{{OrgName}} may also include additional conditions relating to the provision of interoperability elements.