About Helen O.

Helen was just selected Best Lawyers® 2022 “Lawyer of the Year” for Health Care Law in Princeton, Ne Jersey, a distinction awarded to one lawyer with the highest overall peer-feedback for a specific practice area and geographic region. She is also selected to the 2020 & 2021 Super Lawyers® list for Health Care Law in New Jersey, which is issued by Thomson Reuters. Every year since 2018, her law firm has also been included on the “Best Law Firms” in Health Care Law, Princeton, New Jersey list issued by Best Lawyers. Links to a description of the selection methodologies used by the organizations issuing these lists can be found here.

Helen is a corporate and regulatory attorney whose practice for over the last 20 years has focused almost exclusively on advising and representing clients in the health care industry. She is the founding member of Attorneys at Oscislawski LLC, a progressive and forward-thinking law boutique providing high-quality and cost-effective legal representation to its clients. Helen cemented her reputation as a prominent privacy and health information technology attorney through decades of developed experience and working hand-in-hand with C-suite executives and in-house general counsels on how to structure and manage complex data-sharing arrangements in compliance with applicable federal and state laws. She is known to many as a “go-to” attorney for legal guidance and advice on HIPAA; 42 CFR Part 2; Breach Notification laws, as well as state laws regulating the access, use and sharing of medical, health and genetic information. Helen also has substantial experience with helping her clients navigate legal issues when responding to ransomware attacks, data breaches, OCR audit and complaint letters, and return/sanitization of patient data taken by former employees. On the front end, Helen has completed numerous comprehensive HIPAA legal-gap assessments for health care organizations and business associates, including some of the largest health information exchanges (HIEs) in the tri-state area. In 2008, New Jersey Governor Jon Corzine appointed Helen to the New Jersey Health Information Technology Commission (NJ-HITC) to fill the seat designated by statute for “an attorney practicing in this State with demonstrated expertise in health privacy.” N.J.S.A. 26:1A-137(a)2).[statutorily defined]. In 2010, she was reappointed to NJ-HITC by Governor Christie and tapped to serve as Chair of the Privacy and Security Committee for the New Jersey HIT Coordinator. As a trusted advisor, Helen currently represents and advises some of the most cutting edge and sophisticated organizations in the nation, including several large multi-stakeholder collaboratives in the NJ/NY/PA region, as well as a number of burgeoning “big data” innovation projects and initiatives.

Before founding Attorneys at Oscislawski LLC, Helen was a health care attorney with a national law firm for almost a decade where she counseled all types of health care clients on a wide range of legal matters. Helen received her law degree from Rutgers School of Law, with honours, in 1999, and is admitted in New Jersey (since 1999) and Arizona (since 2020). She completed her undergraduate degree at Rutgers University, Douglass College in 1994, with highest honours in her major and high honours overall. She was inducted into Phi Beta Kappa upon graduation.

Helen can be reached at helen@oscislaw.com or 609-385-0833 ext.1.
Disclaimers

- This presentation is for informational purposes only.
- It does NOT, and is not intended to, constitute legal advice.
- Only your attorney can provide assurances regarding the application of this information to your particular circumstances. Attorneys at Oscislawski LLC always recommends you consult with your own counsel.
- The statements, views, and opinions expressed in this presentation and on the following slides are solely those of the presenter, and not those of CHCANYS.
What questions or practical issues would you like to see addressed in the Information Blocking learning sessions from a Compliance and/or IT perspective?

1. Sharing/blocking psychotherapy notes with patients/parents/guardians. Information Blocking rule vs. HIPAA-preemption analysis. Including when they are part of an integrated health record (i.e., not kept separate from the health record). PRIVACY EXCEPTION

2. Latitude of ability to release information for care coordination purposes to non-covered entity PRIVACY EXCEPTION; PROPOSED CHANGES TO HIPAA PRIVACY RULE

3. Examples of patient data that fall under the self-harm clause. Tips on how to implement policy and how to document PREVENTING HARM EXCEPTION; TIP SHEET

4. Implications for behavioral health providers/SUD and BH compliance issues PRIVACY EXCEPTION; TECHNOLOGY (segmentation)

5. Questions surrounding auto-release of results to patient portals e.g., risk of feeding information to a patient portal before provider review. INFORMATION BLOCKING; PREVENTING HARM; INFEASIBILITY

6. What turnaround time frames do you recommend when the org has 2 or more EMRs? ONC FAQ.

7. Staff still need crystal-clear explanations of why common steps (e.g. requiring patient request) are info blocking. REQUEST IS PRE-REQUISITE. ONC FAQ ON PORTALS.

8. Questions surrounding making available full clinical notes. USCDIv2; CONTENT EXCEPTION.

9. How do the functionality of interfaces effect our legal standing. INFEASIBILITY EXCEPTION

10. Sample compliance P&P LEGAL HIE COMPLIANCE LIBRARY
What is “Information Blocking”
“Information Blocking” Definition

45 C.F.R. 171.103(a)(1)

"Information blocking means a practice that —

... is likely to interfere with access, exchange, or use of electronic health information ..."

(unless the practice is required by law or an exception applies)

There are two different knowledge standards ...
Health Care Provider: *Knows*

45 C.F.R. 171.103(a)(3)

“If conducted by a health care provider, such provider *knows* that such practice is unreasonable and is likely to *interfere with* access, exchange, or use of electronic health information . . .”
Developer Certified Health IT & HIEs/HINs: 
*Knows or Should Know*

45 C.F.R. 171.103(a)(2)

“If conducted by a health information technology developer, health information network or health information exchange, such developer, network or exchange *knows, or should know*, that such practice is likely to *interfere with* access, exchange, or use of electronic health information . . .”
ONC Preamble:

“The following hypothetical situations illustrate some (though not all) of the types of practices described above and which would implicate the information blocking provision . . .”
Example #1

**Picking & Choosing Connections**

A health care provider implements locally-hosted certified EHR technology. The technology developer is required to and provides the health care provider with the **capability** to automatically publish its **production endpoints** (i.e., the internet servers that an app must “call” and interact with in order to request and exchange patient data). The health system chooses not to enable this capability, however, and **provides the production endpoint information only to apps it specifically approves**. This prevents other applications—and patients that use them—from accessing data that should be made readily accessible via standardized APIs.
Example #2

Picking & Choosing Referrals

A health care provider *directs its EHR developer to configure* its technology so that *users cannot easily send* electronic patient referrals and associated EHI to *unaffiliated providers*, even when the user knows the Direct address and/or identity (i.e., National Provider Identifier) of the unaffiliated provider.
Example #3

Disabling Patient Portals

Although an EHR developer’s *patient portal* offers the capability for patients to directly *transmit or request for direct transmission of their EHI to a third party*, health care provider *chooses not to enable this capability*. 
Example #4

Delaying Access

A health care provider has the capability to provide *same-day access to EHI* in a form and format requested by a patient or a patient’s health care provider, but *takes several days to respond.*
ONC FAQ: 

Delays & Unnecessary Impediments

**Question:** Are actors (for example, health care providers) expected to release test results to patients through a patient portal or application programming interface (API) *as soon as the results are available to the ordering clinician?*

**Answer:** While the information blocking regulations do not require actors to *proactively* make electronic health information (EHI) available, once a request to access, exchange or use EHI is made actors must timely respond to the request (for example, from a patient for their test results). Delays or other unnecessary impediments could implicate the information blocking provisions. *In practice, this could mean a patient would be able to access EHI such as test results in parallel to the availability of the test results to the ordering clinician.*

[www.healthit.gov/curesrule/faq/are-actors-for-example-health-care-providers-expected-release-test-results-patients-through](http://www.healthit.gov/curesrule/faq/are-actors-for-example-health-care-providers-expected-release-test-results-patients-through)
**Question:** When would a *delay in fulfilling* a request for access, exchange, or use of EHI be considered an interference under the information blocking regulation?

**Answer:** A determination as to whether a delay would be an interference that implicates the information blocking regulation would require a *fact-based, case-by-case assessment of the circumstances*. That assessment would also determine whether the interference is with the legally permissible access, exchange, or use of EHI; whether the actor engaged in the practice with the requisite intent; and whether the practice satisfied the conditions of an exception. Please see 45 CFR 171.103 regarding the elements of information blocking.

*Con’t …*
ONC FAQ: Necessary Delays

**Unlikely to be an Interference**

If the *delay is necessary* to enable the access, exchange, or use of EHI, it is unlikely to be considered an interference under the definition of information blocking.

For example, if the release of EHI is delayed *in order to ensure that the release complies with state law*, it is unlikely to be considered an interference so long as the delay is no longer than necessary.

Longer delays might also be possible, and not be considered an interference *if no longer than necessary*, in scenarios where *EHI must be manually retrieved and moved from one system to another system* (see, for example, 85 FR 25866-25887 regarding the manual retrieval of EHI in response to a patient request for EHI).

Con’t …
Likely to be an Interference

It would likely be considered an interference for purposes of information blocking if a health care provider established an organizational policy that, for example, imposed delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results (see also 85 FR 25842 specifying that such a practice does not qualify for the “Preventing Harm” Exception).

To further illustrate, it also would likely be considered an interference:

- where a delay in providing access, exchange, or use occurs after a patient logs in to a patient portal to access EHI that a health care provider has (including, for example, lab results) and such EHI is not available—for any period of time—through the portal.
- where a delay occurs in providing a patient’s EHI via an API to an app that the patient has authorized to receive their EHI.
**Question:** Do the information blocking regulations (45 CFR Part 171) require actors to *proactively* make electronic health information (EHI) available through “patient portals,” application programming interfaces (API), or other health information technology?

**Answer:** No. There is no requirement under the information blocking regulations to proactively make available any EHI to patients or others *who have not requested the EHI*. We note, however, that a delay in the release or availability of EHI in response to a request for legally permissible access, exchange, or use of EHI may be an interference under the information blocking regulations....

ONC FAQ: Delays per HIPAA or State Law

**Question:** When a state or federal law or regulation, such as the HIPAA Privacy Rule, requires EHI be released by no later than a certain date after a request is made, is it safe to assume that any practices that result in the requested EHI’s release within that other required timeframe will never be considered information blocking? (IB.FAQ26.1.2021JAN)

**Answer:** No. The information blocking regulations (45 CFR Part 171) have their own standalone provisions (see 42 U.S.C. 300jj-52). The fact that an actor covered by the information blocking regulations meets its obligations under another law applicable to them or its circumstances (such as the maximum allowed time an actor has under that law to respond to a patient’s request) will not automatically demonstrate that the actor’s practice does not implicate the information blocking definition.

If an actor who could more promptly fulfill requests for legally permissible access, exchange, or use of EHI chooses instead to engage in a practice that delays fulfilling those requests, that practice could constitute an interference under the information blocking regulation, even if requests affected by the practice are fulfilled within a time period specified by a different applicable law.

www.healthit.gov/curesrule/faq/when-state-or-federal-law-or-regulation-such-hipaa-privacy-rule-requires-ehi-be-released-no
**ONC FAQ:**

**BAA Terms that “Interfere”**

**Question:** Do the information blocking regulations require actors to violate existing business associate agreements in order to not be considered information blockers?

**Answer:** No. The information blocking regulation in 45 CFR part 171 do not require actors to violate business associate agreements (BAA) or associated service level agreements. However, the terms or provisions of such agreements could constitute an interference (and thus could be information blocking) if used in a discriminatory manner by an actor to forbid or limit access, exchange, or use of electronic health information (EHI) that otherwise would be a permitted disclosure under the Privacy Rule.

For example, a BAA entered into by one or more actors that permits access, exchange, or use of EHI by certain health care providers for treatment should generally not prohibit or limit the access, exchange, or use of the EHI for treatment by other health care providers of a patient. See also the section discussing business associate agreements in the Final Rule at 85 FR 25812.

Contract Terms as “Interference”

• “Contracts and agreements can interfere with the access, exchange, and use of EHI through terms besides those that specify unreasonable fees and commercially unreasonable licensing terms.

• A contract may implicate the information blocking provision if it included unconscionable terms for the access, exchange, or use of EHI or licensing of an interoperability element.

Example: requiring a software company that produced a patient access application to relinquish all IP rights to the Actor or agreeing to indemnify the Actor for acts beyond standard practice, such as gross negligence on part of the Actor...”
Compliance To Do: “Interference”

- Identify **practices, policies** and **contract terms** that could be construed as potentially “**interfering with**” access, exchange and use of EHI. Start with:
  - Patient Portal
  - Provider Portal
  - EMR requests for access, exchange and use of EHI
  - Business Associate Agreements

- **Revise language** reflecting impermissible practices:
  - Data sharing agreements and BAAs that treat two types of otherwise similarly-situated requestors differently
  - Unreasonably delays (delays not required by law or absolutely necessary)
  - Unnecessary impediments (signing of consents when not required by law)
  - No blanket delays (e.g., 48 hrs for physician review)
  - Update policies to include asking patients for preference on immediate vs. delay of availability of test results, and preferred access to other EHI
8 Safe Harbors

1. Preventing Harm
2. Privacy
3. Security
4. Infeasibility
5. Health IT Performance
6. Content & Matter
7. Fees
8. Licensing
Preventing Harm
Required Elements Must be Met

- *Reasonable* belief

- The practice will *substantially reduce*

- A “Risk” of “Harm” to a patient or another natural person that would otherwise arise if the access, exchange, or use of EHI were to be granted

- The practice must be *no broader than necessary* to substantially reduce the risk of harm that the practice is implemented to reduce.
Type of “Risk”

The risk of harm must either:

(1) Be determined on an **individualized basis** in the exercise of **professional judgment** by a **licensed health care professional** who has a **current** or **prior clinician-patient relationship** with the patient whose EHI is affected by the determination;

**OR**

(2) **Arise from data** that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.
HIPAA Access Right – 2 Harm Standards

(3) *Reviewable grounds for denial.* A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is *reasonably likely to endanger the life or physical safety of the* individual or another person;

(ii) The protected health information makes reference to another person (unless such other person (who is not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause *substantial harm to such other person*; or

(iii) The request for access is made by the individual’s personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause *substantial harm* to the individual or another person.
Two Harm Standards

What Qualifies as “Substantial Harm”?

“Substantial harm” would have to be serious in nature. Otherwise, the licensed health care professional would be permitted to consider substantial physical, emotional, or psychological harm when making a determination to withhold access under the substantial harm standard. The federal government will defer to the professional judgement of the health care professional in making a determination that “substantial harm” is reasonably likely.

What Qualifies as “Endangering Life or Physical Safety”?

The most commonly cited example of “danger to the life or physical safety” of a patient or another person is when such patient exhibits suicidal or homicidal tendencies. Specifically, if a licensed health care professional determines that an individual exhibits such tendencies and that permitting inspection or copying of some of the individual’s EHI is reasonably likely to result in the individual committing suicide, murder, or other physical violence, then the health care professional may deny the individual access to that information.

Under this standard, a licensed health care professional would NOT be permitted to deny access based on the sensitivity of the health information or the potential for causing emotional or psychological harm.
# How to Make a “Harm” Determination

<table>
<thead>
<tr>
<th>Who is the Requestor?</th>
<th>Does the EHI Reference Another Person?</th>
<th>Required Standard of Harm</th>
<th>Who Determines Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Representative (including “personal representative” under HIPAA).</td>
<td>No</td>
<td>Reasonably likely to cause <strong>substantial harm</strong> to the patient or another person</td>
<td>Individualized determination of harm by licensed health care professional who has a current or prior clinician-patient relationship with the patient</td>
</tr>
<tr>
<td><strong>Patient or Legal Representative</strong></td>
<td>YES</td>
<td>Reasonably likely to cause <strong>substantial harm</strong> to such other person referenced in the EHI</td>
<td>Individualized determination of harm by licensed health care professional who has a current or prior clinician-patient relationship with the patient</td>
</tr>
</tbody>
</table>
| **Patient** | No | Reasonably likely to endanger the life or physical safety of patient or another person | Individualized determination of harm by licensed health care professional who has a current or prior clinician-patient relationship with the patient  
- OR – 
**Arises from Data**  
suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason |
| **Any other requestor who has a “legally permissible” right to access, use or exchange the EHI** | N/A | Reasonably likely to endanger the life or physical safety of patient or another person | Individualized determination of harm by licensed health care professional who has a current or prior clinician-patient relationship with the patient  
- OR – 
**Arises from Data**  
suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason |
Implementation

- **Organizational policy:**
  - Be in writing
  - Be based on relevant clinical, technical, and other appropriate expertise;
  - Be implemented in a consistent and non-discriminatory manner; and
  - Conforms each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use.

- **Individualized Determination:**
  - Based on facts and circumstances known or reasonably believed by the Actor at the time the determination was made and while the practice remains in use;
  - Be based on expertise relevant to implementing the practice consistent with the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through (e) of this section that are applicable to the practice and its use in particular circumstances.
“[W]e are not persuaded that **routinely time-delaying** the availability of broad classes of EHI should be recognized as excepted from the information blocking definition under this exception . . .”

➢ **No evidence** that **routinely delaying** EHI availability to patients in the interest of fostering clinician-patient relationships **substantially reduces danger to life or physical safety of patients or other persons** that would otherwise routinely arise from patients’ choosing to access the information as soon as it is finalized.

➢ **Unless applicable law prohibits** making particular information available to a patient electronically before it has been conveyed in another way, **deference should generally be afforded to patients’ right to choose** whether to access their data as soon as it is available or wait for the provider to contact them to discuss their results.
Sample Use Case: Permissible Delaying of Diagnostic Results

- **Use Case**: Adult Patient (18yo+) requests access to his/her *own* diagnostic results. This would include any and all type of blood work, cancer screenings, pathology, genetic results etc.

- **Applicable Harm Standard**: Reasonably likely to endanger the *life* or *physical safety*.

**Permissible “Preventing Harm” Determination**

- Results *cannot* be withheld due to mere “sensitivity” or potential for *emotional* or *psychological* distress.

- Labs must be released to patient *immediately* when available with no delay *unless* the patient is provided with an opportunity and agreed.

- **Suicide**: If the patient has specifically expressed the intent or desire to *commit suicide* in response to receiving a negative diagnostic result, the patient’s licensed health care professional *may* make an individualized determination that withholding a diagnostic result is reasonably likely to reduce or prevent danger to the life or safety of the patient.

**EXAMPLE**: A patient has advanced cancer, has a prior attempted suicide by intentional overdose and specifically has stated that if the diagnostic result shows progression of the cancer that she would make sure that her “next attempt” to take her own life is successful. The patient’s diagnostic test result reveals rapid progression of the cancer. The licensed health care professional may determine to at least delay the release the diagnostic results to the patient until such results can be relayed to her in person, and mental health support resources can be offered. The patient is entitled to a review of the denial.
Compliance To Do: “Preventing Harm”

- Develop and Implement an **IBR P&P** for Preventing Harm
- **Train** Licensed Health Care Professionals on how to properly make “harm” determinations under the IBR Preventing Harm exception:
  - The two (2) harm standards, and when they can be used. Use Legal HIE Tip Sheet for assistance.
  - Determine if technology supports individualized determinations by Health Care Professionals
- Introduce process to request **patient preferences** re: timing of access to EHI requested.
- **Update HIPAA P&Ps** to address differences between the IBR Preventing Harm Exception and HIPAA (see Legal HIE Whitepaper for further detailed suggestions):
  - Uses & Disclosures of PHI
  - Right to Access
Legal HIE – Sample IBR Policy

Preventing Harm Exception

POLICY: Preventing Harm Exception

CATEGORY: Information Blocking
POLICY TOPIC: Preventing Harm Exception
EFFECTIVE DATE: April 5, 2021

I. POLICY
Actor will not knowingly engage in any act or omission (“Practice”) that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (“Block EHI”) unless Actor is required by law to do so, or Actor engages in Blocking EHI in order to prevent a risk of harm. If Actor determines to Block EHI in order to prevent risk of harm, it shall do so only if Actor holds a reasonable belief that such action will substantially reduce the Risk of Harm to a patient or another natural person that would otherwise arise from the access, exchange, or use of electronic health information. Actor will not Block EHI in any manner that is broader than necessary to substantially reduce the risk of harm that the action is intended to reduce.

II. DEFINITIONS
“Exception” shall mean any one of the eight (8) exceptions to Information Blocking that are set forth in Title 45, Part 171 (Information Blocking), Subparts B & C.
“Licensed Health Care Professional” any person who holds a valid license from a state licensing board to provide health care services to patients.
“Patient” shall mean, for purposes of this policy, a natural person who is the subject of the electronic health information affected by an act or omission that prevents, materially discourages, or otherwise inhibits the access, exchange and/or use of EHI.

III. PROCEDURE
A. Type of Risk:
(1) The risk of harm must either arise from data OR be determined by a licensed health care professional. No other “type of risk” qualifies for purposes of the Preventing Harm Exception and this policy. If the risk does not arise from data or is not determined by a licensed health care professional to exist, in accordance with this policy, then Actor must not Block EHI unless it is otherwise required by law to do so, or another Exception Applies.
(2) Risk Arising from Data:
   a. A “risk” of harm that arises from data must be either known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

b. A known or reasonably suspected “risk” of harm arising from data shall be evaluated and determined by appropriate persons as identified by Actor’s CIO and/or IT Director.

c. Examples:
   o A Patient declining to consent to share 42 CFR part 2 substance abuse treatment information would not render the remainder of the Patient’s record inaccurate based on its incompleteness.
   o Actor may not delay fulfillment of an otherwise feasible and legally permissible request for exchange, access, or use of EHI that is finalized and available to a requestor merely because Actor knows more EHI will become available at some later date.
   o Actor may not Block EHI solely because the Patient might discover error(s) in that EHI.
   o Actor may not routinely and on a “blanket basis” take data coming in from a third-party “off line” to confirm that it is not corrupt, mismatched, or otherwise problematic data – unless Actor has “actual knowledge” or a “reasonable suspicion” that such data could be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason, based on facts known to Actor.
   o Actor may take time to “map” and/or convert data coming in to “structures and standards” used by it. This exception applies to “appropriately tailored practices” for assessing and mitigating risks posed by integration of data from new sources that are not standardized, or that is standardized to non-published, proprietary, or obsolete standards.

(3) Licensed Health Care Professional Determination:
   a. The Licensed Health Care Professional making a “risk” of harm determination for purposes of this policy must have either a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination.
   b. The Licensed Health Care Professional’s determination must be made on an individualized basis in the exercise of professional judgment.
   c. The Licensed Health Care Professional’s determination should either be documented in the EMR or ascertainable from other reliable records already created or being created in connection with the patient’s services at Actor. Licensed Health Care Professional is not required to document different or duplicate documentation of information that is already otherwise already captured in reliable records consistent with other federal and state laws.
Legal HIE – Tip Sheet
Preventing Harm Determinations & Selected Use Cases

Use Case Examples

Patient Request (Adult) – Diagnostic Results

- Use Case: Adult Patient (38yo) requests access to her blood diagnostic results. This would include any and all type of blood work, cancer screening, pathology, genetic tests, etc.
- Harm Standard: Reasonably likely to endanger the life or physical safety.

Permissible Determinations:

- Labs & other diagnostic tests cannot be withheld due to misuse “cryptic” or potential for emotional or psychological distress.
- Labs must be released to the patient immediately when available with no delay unless the patient is provided with an opportunity and agreed to delay the release of the diagnostic result to her/him until a certain event (e.g., review of result by physician).
- Suicide: If the patient has specifically expressed the intent or desire to commit suicide in response to receiving a negative diagnostic result, the patient’s licensed health care professional may make an individualized determination that withholding the diagnostic result under such particular set of facts and circumstances is reasonably likely to reduce or prevent danger to the life or safety of the patient.

EXAMPLE: A patient has advanced cancer, has a prior attempted suicide by intentional overdose and specifically has stated that if the diagnostic result shows propagation of the cancer that she would make sure that her “last attempt” to take her own life is successful. The patient’s diagnostic test result reveals rapid progression of the cancer. The licensed health care professional may determine to at least delay the release of the diagnostic results to the patient until such results can be reviewed by her/him, and mental health support resources can be offered. The patient is entitled to a review of the denial.

- Other Physical Violence: If the patient has specifically expressed the intent or desire to commit physical violence, including homicide, which is reasonably likely to result in danger to the life or physical safety of the patient or another person in response to receiving a diagnostic result, the patient’s licensed health care professional may make an individualized determination that withholding the diagnostic result under such particular facts and circumstances is reasonably likely to reduce or prevent danger to the life or safety of the patient or another person.

EXAMPLE: A male patient has presented to be tested for HIV/AIDS. The patient shared that he suspects that his female partner has been unfaithful to him, contracted the STD, and passed it to him. The patient also has sustained an injury to his partner if the test comes back positive. The patient’s emotional disposition is angry and reclusive. The patient’s diagnostic test result reveals a positive HIV test result. The licensed health care professional may determine at least delay the release of the diagnostic results to the patient until such results can be reviewed by the patient in person, and appropriate interventions can be put in place. The patient is entitled to a review of the denial.

Patient Request (Adult) – Diagnosis of Anorexia Nervosa

- Use Case: Adult Patient (23yo) with diagnosis of anorexia nervosa requests access to her health information.
- Harm Standard: Reasonably likely to endanger the life or physical safety.

Permissible Determinations:

- Health information cannot be withheld from a patient due to “anorexia nervosa” or potential for emotional or psychological distress.
- When a patient exercises the right to access or receive a copy of her/his health information, it must be made available to the patient immediately as soon as it is available to the patient. The patient is provided with an opportunity to agree to a specific time-frame for receipt of such information (i.e., 30 days) or other delay, and has agreed to such time-frame or delay.
- Suicide: If the patient has specifically expressed the intent or desire to commit suicide or engage in self-destructive behaviors which would inevitably lead to death or danger to the patient’s physical safety, the patient’s licensed health care professional may make an individualized determination to withhold certain components of the patient’s health record, no broader than necessary to prevent or reduce danger to the life or safety of the patient.

EXAMPLE: A patient was diagnosed with anorexia nervosa. Patient has a history of going on “food strikes” when she is shown increase in her weight to the point Where it becomes necessary to admit the patient in order to provide her with necessary nutrition and prevent imminent death. The patient has requested a copy of her health information, and it is suspected that she intends in part to reduce her weight to the point where her weight is increasing. Her medical record shows that the patient has gained 15 pounds. The licensed health care professional may determine to withhold the patient’s weight from release to the patient at least until the patient’s health care professional is reasonably assured that appropriate interventions are in place to prevent or lessen the chance of her repeating a life-threatening “food strike.” The patient is entitled to a review of the denial.

Request by “Personal Representative” – EHI References Another Person

- Use Case: Biological father requests electronic access to his newborn’s EHI. The EHI references the biological mother of the EHI.
- Harm Standard: Reasonably likely to cause substantial harm to the patient or another person.

Permissible Determinations:

- HIPAA generally requires a second-party provider to share a patient’s EHI with any person who has authority under applicable law to “act on behalf” of a patient in making decisions related to health care (an oral consent is required if there is suspected abuse, neglect or abandonment involved).
- Abortion: A court order authorizing such right, or a biological father of a minor child who would otherwise have legal authority to access the EHI.
- Substantial Harm: If a patient’s EHI references another person, a health care professional may decline to provide requested EHI to the personal representative if doing so is reasonably likely to cause substantial physical, emotional or psychological harm to such person.

EXAMPLE: The biological father of a newborn requests electronic access to his newborn’s EHI through a patient portal. The newborn’s biological mother’s EHI is referenced in the newborn’s record, and also reveals that the mother had illegal narcotics in her blood during the newborn’s birth. The newborn’s mother and father are not on friendly terms. The father has been verbally abused and disparaged of the mother on multiple fronts. The biological mother is not available to be asked whether it would be permissible to share the newborn’s record containing her EHI, and specifically identifying her drug use, to the father. Additionally, the EHR is not technologically capable of segmenting out and withholding just the mother’s EHI from being sent to a patient portal. In such case, a licensed health care professional has a current and prior clinical-patient relationship with the mother & newborn may make an individualized determination to share the father’s access to the newborn’s EHI if requested (e.g., through the portal) because learning about the mother’s drug use is reasonably likely to cause the mother emotional or psychological harm. The health care professional must offer the mother an alternate manner in which to obtain a copy of his newborn’s EHI where the mother’s EHI can be redacted.

© 2021 Oscislawski LLC

Connecting Healthcare with Legal Excellence®

© 2021 Oscislawski LLC
Legal HIE - Whitepaper
How to Implement Preventing Harm

Whitepaper: Blocking EHI to “Prevent Harm” Under HIPAA & Info Blocking

**ANALYSIS:** Comparing the IB Rule “Preventing Harm” Exception & HIPAA

Although ONC has noted that the Preventing Harm Exception to Information Blocking is intended to “align” with the HIPAA Privacy Rule’s provisions governing denial of access requests by patients and their personal representatives, it differs from HIPAA in very important ways.

First, the Preventing Harm Exception applies requests beyond those received from just patients and/or their personal representatives. HIPAA’s “right of access” grants patients/individuals and their “personal representatives” certain guaranteed rights to inspect and access their PHI. Similarly, the Preventing Harm Exception also covers requests received from patients/individuals and their personal representatives. However, for purposes of Information Blocking, the Preventing Harm Exception may also be considered when responding to any requestor who has a “legally permissible” right to access, use or exchange the EHI. In addition, the Preventing Harm Exception uses the broader term “legal representative” to include persons who “legally act on behalf of” an individual/patient seeking health care decisions. This term includes persons who qualify as a “personal representative” under HIPAA’s definition of such term, as well as persons who do not but are still recognized as a “legal representative” for purposes of Information Blocking Rule and the Preventing Harm Exception.

**ACTION ITEM:** Actors that are also covered entities should review and update their HIPAA P & P’s governing “Uses & Disclosures of PHI” to address the following: (a) a legally-permissible request for PHI may not be “blocked” unless an Information Blocking Exception applies; and (b) a Preventing Harm Exception policy should be considered and, when appropriate, applied in response to EHI requests received from any third-party.

Second, the IB Rule applies a stricter standard for determinations of “harm” by licensed health care professionals than is required by HIPAA. To qualify for the Preventing Harm Exception, the licensed health care professional making a “harm” determination as a basis to deny a patient/individual or his/her legal representative access to EHI must have a current or prior clinician-patient relationship with the patient. In comparison, HIPAA does not expressly require this nexus between the patient/individual and health care professional. Up until now, covered entity providers were permitted under HIPAA to potentially have any practitioner make a determination of “harm” in his/her professional judgment.

**ACTION ITEM:** Actors that are also HIPAA covered entities should review and update their HIPAA P & P’s governing “Right to Access” to address this new requirement by adding that “harm” determinations made for purposes of reviewable denial of requests of access made by a patient/individual may only be decided by licensed health care professionals with a current or prior clinician-patient relationship with the patient/individual whose PHI/EHI is being requested.

Third, the IB Rule applies a second “stricter” standard for “harm” determinations made by licensed health care professionals than is required by HIPAA. Under the Preventing Harm Exception, determinations of “harm” made by a licensed health care professional must be made on an individualized basis. HIPAA does not expressly require such determinations to be made on an individualized basis, only “in the exercise of professional judgment.” As such, covered entity providers were arguably permitted under HIPAA to have a licensed health care professional develop a “blanket policy” based on standard of care and their professional judgment to allow for denial of access to patients under a specific set of facts and circumstances which could warrant it. After the IB Rule goes into effect, this will no longer be permitted.

**ACTION ITEM:** Actors that are also HIPAA covered entities should review and update their HIPAA P & P’s governing “Right to Access” as needed to require “harm” determinations to be made on an individualized basis when necessary to fit under the Preventing Harm Exception.

Finally, under the Preventing Harm Exception, “harm” may be determined by a licensed health care professional or arise out of data that is misidentified, mismatched, corrupt or erroneous. In contrast, HIPAA does not recognize “harm” arising from data, only “harm” that is determined by a licensed health care professional. This is an area of conflict between how HIPAA Privacy Rule and the Information Blocking Rule currently work. Although the “standard of harm” that would apply is the same in both instances when access is requested by the patient individual (i.e. “danger to life or physical safety”), HIPAA states that “a covered entity may not deny a covered entity to deny a patient/individual access to his/her PHI when ‘harm’ is claimed to be out of data but is not otherwise confirmed by a licensed health care professional. As such, a covered entity provider may consider three options:

- **Delay** access instead of denying access completely. If data is misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason but this issue can be corrected, then an actor/covered entity would be permitted to delay providing the requested EHI/PHI to the individual until the data can be corrected. This is allowed under both the IB Rule’s Preventing Harm Exception and HIPAA. In fact, the Preventing Harm Exception requires that an actor not interfere with access to EHI in any manner that is “broadly unreasonable.” Therefore, even though the Preventing Harm Exception would potentially allow for an outright denial of access to EHI for data issues that meet the requisite harm threshold (i.e., danger to life or physical safety of patient or another person), if the data is correctable and corrected, an actor would be expected to fulfill the individual’s request for access at that point in time. Similarly, under HIPAA, a covered entity has up to 30 days to act on a request for access received from the individual. If more than 30 days is needed to correct the data, then the covered entity need only provide the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request.
Legal HIE - Sample Policy

IBR Amendments to HIPAA Access Rights

I. POLICY:
Covered Entity Provider shall inform each person ("the individual") who is a patient or otherwise receiving services from Covered Entity Provider the right to inspect and obtain a copy of his/her protected health information (PHI) maintained in a Designated Record Set (DRS), with the exception of the following:

- Psychotherapy Notes which are recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the Individual’s medical record. Psychotherapy notes specifically do not include the following:
  a. medication prescription and monitoring;
  b. counseling session start and stop times;
  c. the modalities and frequencies of treatment furnished;
  d. results of clinical tests; and
  e. any summary of the following items:
     i. diagnosis, functional status;
     ii. treatment plan;
     iii. symptoms;
     iv. progress; and
     v. progress to date.

- Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

To the extent PHI is maintained in electronic format (i.e., “electronic health information” or “EHI”), the Individual also shall be afforded the right to request a copy of his/her PHI/EHI in an electronic format and format, if readily producible and otherwise in accordance with Covered Entity Provider’s policies governing information blocking. Covered Entity Provider in whole or in part may deny an individual’s request for access to his/her PHI/EHI in accordance with this Policy.

II. PROCEDURES

A. Written Request

1. Any individual who wishes to request access to or a copy of his/her PHI/EHI in the Covered Entity Provider’s DRS may be asked to submit an official request in writing (which may include an electronic written request). Any requirement to submit a request in writing may not interfere with the Individual’s ability to access, use, or exchange EHI, including not “materially discouraging” the individual’s access, use, or exchange of his/her EHI.

2. Covered Entity Provider shall inform the Individual of any request to submit a request in writing. The request may be required to specify the scope of information the Individual wishes to have access to or copies of.

3. Covered Entity Provider may use its “HIPAA Authorization” form to allow the Individual to complete his/her request in writing, but this shall not be required. The process for submitting such request in writing may not serve as a barrier or cause unreasonable delay to the patient being granted access to his/her PHI/EHI.

4. Each Individual shall also be afforded the right to direct Covered Entity Provider to transmit his/her PHI/EHI directly to another person or entity designated by the Individual. The Individual may be asked to submit such request in writing (which may include an electronic request) that clearly identifies the designated person/entity and where to send the PHI/EHI.

5. Covered Entity Provider shall make its written request procedures readily available for Individuals to use to submit access requests. A copy of written request forms shall be made available for pick up in person, by mail, downloaded off Covered Entity Provider’s website or secure portal, e-mailed, or faxed. Covered Entity Provider shall honor the Individual’s preference for how to receive a copy of the request form, or other request procedure.

6. The written request may be submitted to Covered Entity Provider either in person, by U.S. mail, secure fax, secure electronic portal (if available), e-mail, or as a secure, connected Application of the Individual’s choice. Covered Entity Provider shall honor the Individual’s preference for how to submit their request. Use of the Individual’s personal email is not prohibited provided that Covered Entity Provider informs/educates the individual of the risks associated with transmitting his/her PHI through unsecured email, the Individual acknowledges an understanding of these risks, and accepts such risks in using e-mail in connection with exercising his/her access rights.

B. Identity Verification

1. Covered Entity Provider will request at least one form of reliable verification from the Individual (e.g., driver’s license, current address plus DOB) in order to verify their identity. Identity verification and authentication may not create barriers or unreasonably delay the individual obtaining access to his/her PHI, and otherwise must be in accordance with Covered Entity Provider’s policy governing Authentication and Verification for Person/Entity.

---

1 Note: The Privacy Act requires a covered entity to undertake reasonable steps to verify the identity of an individual before the entity discloses PHI to that individual. The guidelines in this document provide examples of reasonable steps for verification. Covered Entity Provider should consider the context in which the request is made and the level of risk involved in granting access based on the verification process.
Privacy Exception
Four (4) Possible Sub-exceptions

1. Precondition Not Satisfied

2. Health IT Developer of Certified Health IT Not Covered by HIPAA

3. Denial Of Individual Right Access Consistent with Privacy Rule 164.524(a)(1) & (2)

4. Respect Individual Request to Not Share Info

Must meet All Elements of at least one Sub-exception
1. Precondition Not Satisfied (PNS)

State or Federal law requires *one or more preconditions* for providing access, exchange, or use of EHI that have not been satisfied. For example, federal or state law requires prior written consent:

- 42 CFR Part 2 records
- Substance abuse treatment records
- Mental Health records
- HIV/AIDS information
- STD information
- Genetic Information
- Minor’s emancipated care
Precondition Not Satisfied (PNS)

In order to qualify for the PNS sub-exception, additional requirements must be met:

- Documentation
- Consent or Authorization efforts
- Laws of Multiple States
PNS: Documentation Requirement

Actor’s practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either:

- Conforms to Actor’s organizational policies & procedures that:
  - Are in writing;
  - Specify the criteria to be used by the actor to determine when the precondition would be satisfied and, as applicable, the steps that Actor will take to satisfy the precondition;

  and

  - Are implemented by Actor, including by providing training on the P&P.

OR

- Documented by Actor, on a case-by-case basis, identifying the criteria used by Actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met.
If the precondition relies on the provision of a consent or authorization from an individual and Actor has received a version of such a consent or authorization that does not satisfy all elements of the precondition required under applicable law, Actor must:

- Use reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or provide other reasonable assistance to the individual to satisfy all required elements of the precondition;

AND

- Not improperly encourage or induce the individual to withhold the consent or authorization.
For purposes of determining whether Actor’s P&Ps and actions satisfy the requirements of paragraphs (b)(1)(i) and (b)(2) above when Actor’s operations are subject to multiple laws which have inconsistent preconditions, they shall be deemed to satisfy the requirements of the paragraphs if the Actor has adopted uniform Privacy P&Ps to address the more restrictive preconditions.
2. Certified/Health IT Developer Not Covered by HIPAA

N/A
3. Denial of Right of Access (HIPAA)

If an individual requests EHI under the HIPAA Privacy Rule’s right of access provision under 45 CFR 164.524(a)(1), the practice must be consistent with 45 CFR 164.524(a)(2):

- Access rights limited to PHI maintained in a Designated Record Set
- Can deny Psychotherapy Notes
- Can deny Info compiled in anticipation of legal action (e.g., civil; criminal; administrative)
- Hospitals under contract/direction of correctional institution can deny inmate request if would jeopardize health, safety, security, custody, or rehabilitation of inmate or other inmates, or safety;
- Research restrictions
- Privacy Act restrictions
- Promise of Confidentiality to third-party source
**Question:** Does the “electronic health information” definition’s exclusion of *psychotherapy notes* apply to notes of sessions conducted by a type of mental health professional other than a psychiatrist? (IB.FAQ16.1.2021JAN)

**Answer:** It depends. To the extent the content of any particular note meets the definition of “psychotherapy notes” in the HIPAA Rules (see 45 CFR 164.501), that note would be considered a psychotherapy note for purposes of information blocking. The information blocking regulations do not specify types of health care providers to be mental health professionals for purposes of applying the “psychotherapy notes” definition under the information blocking regulations. Thus, all notes that are “psychotherapy notes” for purposes of the HIPAA Rules are also “psychotherapy notes” for purposes of the information blocking regulations in 45 CFR part 171, and are therefore excluded from the definition of EHI for purposes of the information blocking regulations.

**Psychotherapy notes** means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.

*Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

4. Respecting Individual’s Request for Restrictions

- **Individual requests** that Provider not grant such access, exchange, or use of Individual’s EHI. Cannot be any improper encouragement or inducement of the request by the Provider;

- Must **document** the Individual’s request for restriction within a reasonable time period;

  and

- Practice must be **implemented** in a **consistent** and **nondiscriminatory** manner.
Actor may **terminate** an individual’s request for a restriction to not provide such access, exchange, or use of the individual’s EHI **ONLY if:**

- The individual agrees to the termination in writing or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented by Actor; **OR**
- Actor informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual’s EHI except that such termination is:
  - Not effective to the extent prohibited by applicable Federal or State law;

  **and**

  - Only applicable to EHI created or received after Actor has so informed the individual of the termination.
Compliance To Do: Privacy

- Develop and Implement an ***IBR P&P*** for Privacy
- Identify **federal and state laws** requiring a precondition (e.g., consent; parental rights to minor’s rights) to access, use and exchange of EHI.
- Develop **detailed procedures** “specifying criteria used” to determine when required precondition is satisfied as a matter of law **and** train workforce on same **OR** develop procedure for making such determinations on case-by-case basis and documenting.
- Review **consent P&Ps**, and revise as needed to address consent requirements in response to Requestor seeking access to EHI:
  - Do not require consent when not required as matter of law
  - Must make *reasonable efforts* to help obtain consent when required
  - Do not improperly encourage or induce person to withhold consent
  - If operating in multiple states, develop uniform P&P to allow most restrictive provisions to apply in all states of operation
- **Update HIPAA P&P** re: Patient Requests for Restrictions to include IBR requirements.
- **Follow HIPAA for denials of Right of Access under 164.524(a)(1)&(2)**
Legal HIE – Sample Policy

Privacy Exception

POLICY: Privacy Exception

CATEGORY: Information Blocking

POLICY TOPIC: Privacy Exception

EFFECTIVE DATE: April 5, 2021

I. POLICY

Actor will not knowingly engage in any act or omission (“Practice”) that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (“EHI”) unless Actor is required by law to do so, or Actor must block EHI in order to protect the privacy of electronic health information (EHI). If Provider decides to Block EHI in order to protect the privacy of EHI, it shall do so only in accordance with this policy and its related procedures.

II. PROCEDURE

A. Precondition Not Satisfied

(1) If state or federal law requires one or more preconditions (e.g., consent) to be satisfied for providing access, exchange, or use of EHI, Actor may Block EHI if all of the requirements of this Subsection “A” are met.

(2) A Practice which would Block EHI may be satisfied to the applicable precondition not satisfied. Actor shall refer to its current HIPAA and other related privacy policies for detail on the specific preconditions required by federal and state laws governing the access, exchange, and use of the following type of EHI (or applicable):

a. Federal Law:
   - Substance Use Disorder Patient Records (42 C.F.R. Part 2);
   - HIPAA Privacy Rule (45 CFR Part 164, Subpart E);
   - Title X (Family Planning) records;
   - WIC records;
   - FERPA records;
   - ADDITIONAL FEDERAL LAW CATEGORIES, AS NEEDED

b. State Law:
   - HIV/AIDS Information;
   - Sexually Transmitted Diseases;
   - Drug & Alcohol Treatment records of state-licensed facilities & programs;
   - Mental Health Treatment records of state-licensed facilities & programs;
   - Genetic Information;
   - Minors’ records;
   - Legal Representatives;
   - Domestic Abuse;
   - ADDITIONAL STATE LAW CATEGORIES, AS NEEDED

(3) If a certain legal precondition relies on the provision of a signed consent or authorization from an individual, and Actor has received a version of such a consent or authorization that does not satisfy all elements under applicable law, Actor shall:

a. Use reasonable efforts within its control to provide the Individual with a consent or authorization form that satisfies all required elements of the applicable law, or provide other reasonable means to the Individual to satisfy all required elements of the consent precondition under applicable law; and

b. Not improperly encourage or induce the Individual to withhold the consent or authorization.

(4) A Practice which would Block EHI must be implemented in a consistent and non-discriminatory manner. This means that Actor shall not:

a. Engage in any Practice in a different manner for similarly-situated requestors (e.g., Block EHI for one requestor, but not Block EHI for a different but similar requestor);

b. Consider whether the requestor is or might be a future competitor of Actor; or

c. Consider whether Actor can charge requestor a certain fee.

(5) Actor may either:

a. Conform a Practice which would Block EHI to its written organization-wide policies and procedures that:

   i. Specify the criteria to be used to determine when a precondition under applicable federal or state law would be satisfied and, as applicable, the steps that Actor will take to satisfy the precondition; and

   ii. Describe how such policies and procedures are implemented, including by providing workforce training;

   OR

b. Document a Practice which would Block EHI on a case-by-case basis, identifying the criteria used to determine when the applicable precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met.

(6) For purposes of determining whether Actor’s privacy policies and procedures and actions satisfy the requirements of this Subsection when Actor’s activities are subject to multiple state laws which have inconsistent precondition requirements, Actor may adopt uniform privacy policies and procedures which apply—across the board—the more restrictive preconditions required under state law. Otherwise, the precondition required by the applicable state law must be applied to the specific Practice in each respective state.
Legal HIE Whitepaper
Minors’ Consent Rights

FEDERAL LAW

HIPAA Privacy Rule

As a general rule, the HIPAA Privacy Rule provides that if under applicable law a parent, guardian or other person acting in loco parentis (the “Parent”) has authority to act on behalf of an unemancipated minor in making decisions related to health care, a covered entity health care provider must treat such parent or legal guardian as the minor’s “Personal Representative” with respect to PHI relevant to such personal representation. However, there are exceptions to this general rule. Specifically, a Parent may NOT be treated as a Personal Representative of the minor, and the minor has the authority to “stand in his/her own shoes” for purposes of the HIPAA Privacy Rule. IF:

(1) State or other law permits the minor to consent to the health care service and:
  - The minor consents to a health care service (regardless of whether the consent of the Parent might also have been obtained); and
  - The minor has not requested that the Parent be treated as his/her Personal Representative.

(2) The minor may lawfully obtain such health care service without the consent of his/her Parent and:
  - the minor consents;
  - or
  - a court or another person authorized by law consents to such health care service.

(3) The Parent agrees to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(4) In addition to (1), (2) & (3) above, a covered entity may elect not to treat a Parent as the minor’s Personal Representative if the covered entity provides in the exercise of professional judgment, decides that it is not in the best interest of the child to treat the Parent as the minor’s Personal Representative because of a reasonable heighten (a) the minor has been or may be subjected to domestic violence, abuse, or neglect by such Parent, OR (b) treating the Parent as the Personal Representative could otherwise endanger the Minor.

*45 CFR 164.502(d)(3)(i)(B). HIPAA expressly allows the covered entity to make this decision “without regard to State law.”

© 2021 Legal Health Information Exchange. All rights reserved.

Whitepaper: Analyzing Minors’ Consent Rights Under HIPAA & State Law

The HIPAA Privacy Rule also provides three additional scenarios which control when a Parent may access or receive a copy of a minor’s PHI:

- If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity health care provider may disclose, or provide “access rights” in accordance with 45 CFR 164.524 to PHI about an unemancipated minor to the Parent (in accordance with such law).

- If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity health care provider may not disclose, or provide access in accordance with 45 CFR 164.524 to PHI about an unemancipated minor to the Parent (in accordance with such law); and

- Where the Parent is not being treated as the Personal Representative of the Minor (because of reason (1), (2) or (3) as described above) and there is no applicable “access rights” provision under State or other law, including case law, a covered entity health care provider may provide or deny access under 45 CFR 164.524 to the Parent if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

The foregoing HIPAA analysis framework must be applied to determine whether a Parent is permitted access to the Minor child’s PHI based on state or other federal law.

42 C.F.R. Part 2 (“Part 2”)

A Minor’s Part 2 information may not be disclosed to a Parent without the consent of the Minor. HIPAA provides that “[i]f, and to the extent, prohibited by an applicable provision of State or other law... a covered entity may not disclose, or provide access in accordance with 45 CFR 164.524 to protected health information about an unemancipated minor to a parent or legal guardian...” The Part 2 regulations expressly prohibit the Minor’s Part 2 information from being disclosed to the Parent when the Minor has exercised his/her right and authority under Part 2 to consent to substance abuse disorder treatment from a Part 2 provider. Therefore, any individual or entity that meets the definition of a “Part 2 Program” and is “federally assisted” must follow this restriction. Likewise, any individual who or entity that receives (a “recipient”) a Minor’s Part 2 information from a Part 2 Program with a re-disclosure notice accompanying such information (as is required by 42 CFR 2.32) must also treat those records in accordance with Part 2’s requirements.

- For purposes of Part 2, “Minor” is defined as: “an individual who has not attained the age of majority specified in the applicable state law, or if no age of majority is specified in the applicable state law, the age of 18 years.” 42 CFR 2.11

© 2021 Legal Health Information Exchange. All rights reserved.

Disclaimer: This text is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts. Do not rely on this text to make any decision which requires the advice of an attorney. Last updated March 2021.
Security  Infeasibility
3 Possible Sub-Exceptions

1. **Uncontrollable events**: Actor 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.

2. **Segmentation**: Actor cannot fulfill the request for access, exchange, or use of EHI because Actor cannot unambiguously segment the requested EHI that cannot be made available due to:

   (i) patient’s preference (refuses to sign consent),

   (ii) due to federal or state law preventing it, or

   (iii) falls within Preventing Harm Exception.

3. **Infeasibility Under The Circumstances**
“Infeasibility Under the Circumstances”

Contemporaneous Written Record or Other Documentation demonstrates consideration of the following factors supporting the determination:

1. The type of EHI and the purposes for which it may be needed;
2. The cost to Actor of complying with the request in the manner requested;
3. The financial and technical resources available to the Actor;
4. Whether the Actor’s practice is non-discriminatory and the Actor provides the same access, exchange, or use of EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
5. Whether the Actor owns or has control over a predominant technology, platform, HIE, or HIN through which EHI is accessed or exchanged; and
6. Why the Actor was unable to provide access, exchange, or use of EHI consistent with the [Content & Manner Exception].

Shall NOT consider whether the manner requested:

1. Would have facilitated competition with Actor; and/or
2. Prevented Actor from charging a fee or resulted in a reduced fee.
Legal HIE Tool: Decision Tree & Documentation

FORM: Infeasibility Under the Circumstances

Unassessable Event: Is there an unassessable event that makes it impossible to fulfill the request?

- YES STOP. Actor may claim Infeasibility Exception & Block HIE for duration of the event.
- NO (continue)

Segmentation: Is it technologically impossible to unsegmentally reaggregate the HIE requested from other EHRs that cannot be released because:

- The individual has refused to sign a consent to release when it is legally required for disclosure, or has requested their information not be shared in this manner, and the Actor has licensed this;
- Federal or state law providers from being disclosed; or
- Those would be “intentional actors” to the individual or another person if request is fulfilled in manner requested (Clinical Document Architecture or Logical Observation Identifier)

- YES STOP. Infeasibility Exception. Privacy Exception. Personal Use Exception.
- NO (continue)

Infeasibility Under the Circumstances:

Document the Infeasibility Factors (REQUIRED):

1. Type of HIE Requested:

2. Purpose(s) for which HIE is requested needed:

3. Cost to the Actor of compiling with the request in the manner requested:

4. The financial and technical resources available to the Actor:

5. Does Actor provide the same access, exchange, or use of HIE to its own companies, or to contractors, suppliers, partners, and other persons with whom it has a business relationship?

- NO Yes. Explain why the circumstance is different here:

6. Can Actor own or control the preexisting technology platforms, health information exchange, or through a network through which HIE is accessed or exchanged?

- NO Yes. Explain why that control does not allow Actor to own or provide HIE.

B. Is it feasible to fulfill the request for HIE in another manner?

1. Can necessary security practices be met to address identified security risks?

- NO STOP. See Security Exception.
- YES (continue)

2. Are there maintenance, improvement or performance issues with the health IT?

- YES STOP. See Health IT Exception.
- NO (continue)

3. Have all other required preconditions under law been satisfied?

- NO STOP. See Privacy Exception.
- YES (continue)

4. Should access be denied based on Actors right to deny access rights under HIPAA?

- YES STOP. See Privacy Exception.
- NO (continue)

5. If requestor asking for more than USC99 data (before May 2, 2022), can Actor:

- NO STOP. Provide requestor with any HIE data requested.
- YES STOP. Provide requestor with HIE data requested.
- NO (continue)

- Segment USC99 data from other EHR and only release USC99 data?

- YES STOP. Provide requestor with USC99 data.
- NO (continue)

C. Is it feasible to fulfill the request for HIE in an alternative manner?

1. Can Actor use technology certified to standards(ies) adopted in 45 C.F.R. Part 170 - “Health Information Technology Standards, Implementation Specifications, and Certification Criteria and Certification Programs for Health Information Technology” that is specified by requestor to fulfill the USC99 data requested?

- YES STOP. Provide requestor with USC99 HIE data in the alternative manner.
- NO (continue)

Actor must provide Requestor with written response within 10 business days describing the reasons why it is infeasible for Actor to fulfill the request.
Must Consider the Manner Exception

❖ **Manner Requested:** Actor must fulfill a request described in paragraph (a) of this section *in any manner requested*, unless Actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

❖ **Alternative Manner:** Actor must fulfill the request *without unnecessary delay* in the following order of priority, starting with first and only proceeding to the next consecutive alternative if Actor is technically unable to fulfill the request in the manner identified in a paragraph:

- Using technology certified to standard(s) adopted in part 170 that is specified by the requestor
- Using content and transport standards specified by the requestor and published by:
  - (1) The Federal Government; or
  - (2) A standards developing organization accredited by the American National Standards Institute.
- Using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.
Documentation Requirement:

If Actor does not fulfill a request for access, exchange, or use of EHI for any of the qualifying reasons, Actor must, within ten (10) business days of receipt of the request, provide to the requestor in writing the reason(s) why the request is infeasible.
NOTICE OF INFEASIBILITY
(pursuant to 45 CFR 171.204(b))

Data Request Received: ___/___/20___

Name of Requestor: ____________________________

Scope of EHI Requested: _______________________

Purpose(s) for which EHI is requested/needed: ____________________________

Date of this Notice of Infeasibility: ___/___/20___ (within 10 business days of request)

YOUR REQUEST FOR ACCESS, EXCHANGE, OR USE OF EHI MAINTAINED AND/OR CONTROLLED BY [ACTOR NAME] IS DENIED DUE TO THE INFEASIBILITY OF FULLFILLING THE REQUEST FOR THE FOLLOWING REASON(S) (see “checking” boxes):

☐ There is an “Uncontrollable Event” that makes it infeasible to fulfill the request.

☐ It is technologically infeasible to unambiguously segment the EHI requested from other EHI that cannot be released because:

☐ The individual has refused to sign a consent to release when it is legally required for disclosure, or has requested that their information not be shared in this manner, and we have honored this request.

☐ Federal or state law prohibit it from being disclosed to requestor.

☐ There would be “Substantial Harm” to the individual or another person if request is fulfilled in manner requested.

☐ It is infeasible to fulfill the request in manner asked because:

☐ Necessary security practices cannot be met to address identified security risks.

☐ There are maintenance, improvement, or performance issues with the health IT.

☐ Preconditions under state or federal law have not been satisfied.

☐ Access is being denied based on [Actors]’s right to deny access rights under HIPAA.

☐ Requester asking for more than UCDM data (before May 3, 2023), and we are unable to provide requestor with all EHI requested, or segment EHI to just provide USCDI data.

☐ It is infeasible to fulfill the request in an alternative manner because:

☐ Actor is unable to provide the requested EHI using technology certified to standards specified by requestor; and

☐ Actor is unable to meet content and transport standards specified by requestor; and

☐ Actor is unable to use an alternative machine-readable format to furnish the USCDI/EHI data requested.
Compliance To Do: Infeasibility

- Develop and Implement an **IBR P&P** for Infeasibility

- Use the Legal HIE **Decision Tree Tool** to evaluate new 
  EHI requests under the Infeasibility Exception and 
  document decisions.

- Use a **“Notice of Infeasibility”** to inform a Requestor 
  when a decision is made to deny access, exchange or 
  use of EHI due to infeasibility. Ensure that decision are 
  consistent and do **not** discriminate.
Legal HIE – Sample Policy

Infeasibility Exception

POLICY: Infeasibility Exception

CATEGORY: Information Blocking

POLICY TOPIC: Infeasibility Exception

EFFECTIVE DATE: April 3, 2021

I. POLICY

Actor will not knowingly engage in any act or omission (“Practice”) that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (“EHI”) unless Actor is required by law to do so, or Actor is excused from responding to requests that are infeasible for Actor to fulfill. If Actor determines to Block EHI due to the infeasibility of responding to the request, Actor shall do so only in accordance with this policy and its related procedures.

II. PROCEDURE

A. Uncontrollable Events

(1) Actor is permitted to Block EHI if an Uncontrollable Event makes it impossible for Actor to fulfill a request for access, exchange, or use of EHI.

(2) For purposes of this policy, an “Uncontrollable Event” includes any:

- natural or man-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.

(3) Actor may Block EHI pursuant to this Subsection A only for the duration of time that the Uncontrollable Event persists. Once an Uncontrollable Event passes, Actor must fulfill the request for access, exchange, or use of EHI unless:

a. Actor cannot fulfill the request due to an inability to “unambiguously segment” requested EHI from other EHI which cannot be shared, as set forth in Subsection “B”; or
b. Actor cannot fulfill the request because response is “infeasible under the circumstances,” as set forth in Subsection “C”; or
c. Another Exception applies.

B. Segmentation

(1) Actor may Block EHI if Actor cannot unambiguously segment requested EHI from other EHI that:

- cannot be made available due to an individual’s expressed preference to not share particular EHI either generally, or with requestor specifically;
- cannot be made available by law; or
- may be withheld in accordance Actor’s “Preventing Harm Exception” policy.

(2) Actor will identify and continue to assess feasible implementation of industry best practices for data segmentation solutions including, but not limited to, as set forth in the HL7 Version 3 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, Part 1: CDA R2 and Privacy Metadata Reusable Content Profile, May 16, 2014 standard for § 179.205(a)(1) (HL7 DS4P standard), which describes the technical means to apply security tags to a health record and data at the document-level, the section-level, or individual data element-level. The HL7 DS4P standard also provides a means to express obligations and disclosure restrictions that may occur for the data.

C. Infeasible Under the Circumstances

(1) Actor is permitted to Block EHI if it is “Infeasible under the circumstances” for Actor to provide access, exchange, or use of EHI.

(2) Actor shall demonstrate through a contemporaneous written record or other documentation Actor’s consistent and non-discriminatory consideration of the following “Infeasibility Factors” that lead to a determination that complying with the request is infeasible under the circumstances:

- The type of EHI and the purpose for which it may be needed;
- The cost to the Actor of complying with the request in the manner requested;
- The financial and technical resources available to the Actor;
- Whether the Actor’s practice is non-discriminatory and the Actor provides the same access, exchange, or use of EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

1 Ref. 35 FED. REG. 25643, 25706 (May 1, 2020). The DS4P standard enables sensitive health information to be exchanged electronically with secure tags in a standardized format and ONC has encouraged health IT developers to include DS4P functionality and make certification of their health IT to those claims in order to support these uses. Compliance with current state and federal privacy laws that protect sensitive health information. ONC notes that implementing a standard that allows for increased predictability in security tagging of sensitive health information would allow for the interoperable exchange of this information to support a wide range of privacy enforcement cases.
Content & Manner
Content
§171.301(a)

➢ Up until **October 5, 2022** – Actor may elect to **only** respond to a request to access, exchange, or use EHI identified by the data elements represented in the **USCDI standard**

➢ **On & after** October 6, 2022, Actor **must** respond to a request to access, exchange, or use of **FULL EHI** (defined in §171.102)
Provider must fulfill a request described in paragraph (a) of this section in any manner requested, unless provider is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

If Actor fulfills a request in any manner requested:

(A) Any fees charged by Actor in relation to fulfilling the response are not required to satisfy the exception in § 171.302 (Fees Exception);

and

(B) Any license of interoperability elements granted Actor in relation to fulfilling the request is not required to satisfy the exception in § 171.303 (Licensing Exception).
Alternative Manner
§171.301(b)(2)

Provider must fulfill the request *without unnecessary delay* in the following order of priority, starting with first and only proceeding to the next alternative if technically unable to fulfill the request in the manner identified in each progressive option:

- Using technology certified to standard(s) adopted in part 170 that is specified by the Requestor
  - □ Yes (stop. Produce EHI in this manner) □ No (proceed)

- Using content and transport standards specified by the requestor and published by: (1) The Federal Government; or (2) A standards developing organization accredited by the American National Standards Institute.
  - □ Yes (stop. Produce EHI in this manner) □ No (proceed)

- Using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.
  - □ Yes (Produce EHI in this manner) □ No (Infeasibility Exception may apply)

- Any fees charged in relation to fulfilling the request are required to satisfy the Fees Exception.
- Any license of interoperability elements granted in relation to fulfilling the request is required to satisfy the Licensing Exception.
Compliance To Do: Content & Manner

- Develop and Implement an IBR P&P for Content & Manner

- Inform Requestors that only USCDI data must be provided through Oct 5, 2022. Include contractual language in BAAs and other Data Sharing Agreements including this restriction.

- Determine whether USCDI data can be segmented from non-USCDI data. If not, provider may assert the Infeasibility Exception.

- Create a process for determining whether the Manner being requested is technically feasible to produce. Use checklist to respond to Requestors accordingly.
Legal HIE – Sample Policy
Content & Manner Exception

I. POLICY
Actor will not knowingly engage in any act or omission (“Practice”) that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (“Block HIE”) unless Actor is required by law to do so, or Actor meets the Content and Manner Exception. Actor may limit the Content of its response to a request to access, exchange, or use EHI, and the Manner in which it fulfills a request to access, exchange or use EHI, provided Actor does so in accordance with this policy, and its related procedures.

II. PROCEDURE
A. Content Exception

(1) USCDS Data. Beginning April 6, 2021 up until October 5, 2022, Actor is required to only respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements in the United States Core Data for Interoperability (USCDI), as may be updated from time to time. See www.healthIT.gov/interoperability/uscdi-data-interoperability- médica.

(2) Full EHI. On and after October 6, 2022, Actor must respond to a request to access, exchange, or use of full EHI, which is defined to mean: electronic protected health information (ePHI) to the extent that such ePHI would be included in a designated record set (DSR), regardless of whether the group of records are used or maintained by or for a HIPAA covered entity, but not including (i) psychotherapy notes (as defined in 45 CFR 164.501); or (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

B. Manner Exception

(1) Actor must fulfill a request for Content, as described in Subsection “A” of this policy, in any manner requested, unless Actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

(2) “Technically unable” shall mean that Actor cannot fulfill a request for access, exchange, or use EHI due to technical limitation. The standard for “technically unable” is not met if Actor is technically able to fulfill the request, but chooses not to fulfill the request in the manner requested due to cost, burden, or similar justifications.

(3) If an Actor fulfills a request in any manner requested (i.e., NOT in an alternative manner):

i. Any fees charged by the Actor in relation to fulfilling the response are not required to satisfy Actor’s policy governing the Fees Exception; and

ii. Any license of interoperability elements granted by the Actor in relation to fulfilling the request is not required to satisfy Actor’s policy governing the Licensing Exception.

Actor may negotiate agreements in any manner requested with whatever terms the Actor chooses and at the “market” rate.

(4) Alternative manner: If Actor does not fulfill the request described in Subparagraph “A,” in any manner requested because it is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the Actor must fulfill the request in an alternative manner, as follows:

i. The Actor must fulfill the request without unnecessary delay in the following order of priority, and only proceeding to the next consecutive alternative manner if Actor is technically unable to fulfill the request in the manner identified:

   ➢ Using technology certified to standard(s) adopted in 45 C.F.R. Part 170 – “Health Information Technology Standards, Implementation Specifications, and Certification Criteria and Certification for Programs for Health Information Technology” that is specified by the requestor;

   ➢ Using content and transport standards specified by the requestor and published by: the federal government, or a standards-developing organization accredited by the American National Standards Institute (ANSI);

   ➢ Using an alternative machine-readable format, including the means to interpret the EHI agreed upon with the requestor.

ii. Any fees charged by Actor in relation to fulfilling a request for access, exchange, or use of EHI in an alternative manner are required to satisfy the Fees Exception, and Actor shall follow its policy governing the same.

iii. Any license of interoperability elements granted by the Actor in relation to fulfilling a request for access, exchange, or use of EHI in an alternative manner is required to satisfy the Licensing Exception, and Actor shall follow its policy governing the same.

(5) If the burden on Actor for fulfilling a request for access, exchange, or use of EHI is so significant that Actor is looking to not to fulfill the request at all, Actor would be required to follow the conditions of and seek coverage under the Infeasibility Exception, as set forth in its policy governing the same.
Elements of the Exception

Fees a Actor charges **must** be —

(i) Based on **objective** and **verifiable criteria** that are uniformly applied for all similarly-situated classes of persons or entities and requests;

(ii) Reasonably related to the **Actor’s costs** of providing the type of access, exchange, or use of electronic health information to, or at the request of, the person or entity to whom the fee is charged;

(iii) **Reasonably allocated** among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported; and

(iv) Based on costs **not otherwise recovered** for the same instance of service to a provider and third party.
Elements of the Exception

The fees Actor charges must **NOT** be based on—

(i) 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;

(ii) *Sales, profit, revenue*, or *other value* that the requestor or other persons derive or may derive from the access, exchange, or use of the EHI;

(iii) *Costs* the Actor incurred due to the health IT being designed or implemented in a *non-standard way*, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the electronic health information;

(iv) *Costs* associated with *intangible assets* other than the actual development or acquisition costs of such assets;

(v) *Opportunity costs* unrelated to the access, exchange, or use of EHI; or

(vi) Any costs that led to the creation of *intellectual property*, if the Actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.
Excluded Fees

This exception does **not apply** to—

1. A **fee prohibited by 45 CFR 164.524(c)(4) of HIPAA Privacy Rule**;

2. A fee based in any part on the **electronic access** of an individual’s EHI by the individual, their personal representative, or another person or entity designated by the individual;

3. A **fee to perform an export of EHI** via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their EHI; and

4. A **fee to export or convert data** from an EHR technology that was not agreed to in writing at the time the technology was acquired.
**Question:** Are contractual fees for the export of electronic health information (EHI) using technology that is not certified to 45 CFR 170.315(b)(10) enforceable if the fees were agreed to prior to the applicability date of the information blocking provision?

**Answer:** Yes, but only to the extent that the fees for the EHI export comply with the “Fees Exception” (45 CFR 171.302). For example, if the fees to export or convert data from the technology were not agreed to in writing at the time the technology was acquired, then the “Fees Exception” would not be available and such fees could implicate the information blocking definition unless another exception applies (45 CFR 171.302(b)(4)).

Note that if the EHI export would be performed using health IT certified under the ONC Health IT Certification Program (45 CFR Part 170) to the “EHI Export” certification criterion (45 CFR 170.315(b)(10)), a fee that is charged to perform such export for purposes of switching health IT or to provide patients their electronic health information (45 CFR 171.302(b)(3)) would not qualify for the “Fees Exception”.

www.healthit.gov/curesrule/resources/information-blocking-faqs
Compliance To Do: Fees

- Develop and Implement an **IBR P&P** for Fees

- Develop a **process** for reviewing fee provisions in applicable agreements to ensure they meet the IBR Fees Exception when required.

- **Review & update HIPAA P&P** re: Right of Access (specifically, re: charging a patient or personal representative any fee for access to EHI).
LEGAL HIE – Sample Policy

FEES EXCEPTION

POLICY: Fees Exception

CATEGORY: Information Blocking

POLICY TOPIC: Fees Exception

EFFECTIVE DATE: April 5, 2021

I. POLICY

Actor’s practice of charging a fee, including a fee that results in a reasonable profit margin for accessing, exchanging, or using electronic health information (EHI) will not be considered prohibited Information Blocking when the practice meets the conditions of and is accomplished in accordance with this policy and its related procedures.

II. SCOPE

A. This Fees Exception policy does not apply, and does not offer an Information Blocking “safe harbor,” to the following:

1. A fee prohibited by the HIPAA Privacy Rule under 45 CFR 164.524(e)(3) in connection with an individual exercising his/her right to request access, inspection or a copy of EHI maintained in Actor’s Designated Record Set, including a summary copy if agreed;

2. A fee in any part on the Electronic Access of an individual’s EHI by the Individual, their Personal Representative, or another person or entity designated by the Individual;

3. A fee to perform an export of EHI via the capability of Health IT certified to [170.315(b)(10)] for the purposes of switching health IT or to provide patients their EHI;

4. A fee to export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

B. Actor shall not be required to follow this Fees Exception policy where requester asks Actor to fulfill a request in a manner which requires non-standard design or implementation and agrees to the fee associated with Actor fulfilling such request in the manner requested (i.e., not as an alternative manner), all in accordance with Actor’s Contract & Support Exception policy. Any such fee charged to a requester must still comply with applicable HIPAA exceptions:

- Prohibiting the “sale” of PHI (see policy attached as “Exhibit A”); and
- On fees that may be charged when the requester is the Individual (or Personal Representative) exercising his/her right to access, inspect or receive a copy of his/her electronic PHI maintained in a Designated Record Set (see HIPAA policy attached as “Exhibit B”)

III. PROCEDURE

A. Permissible Fees

Any fee charged for access, exchange, or use of EHI shall:

1. Be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;

2. Be reasonably related to Actor’s costs of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged;

3. Be reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported;

4. Be based on costs not otherwise recovered for the same instance of service to a provider and third party;

5. Not otherwise prohibited or as described in III.B. of this policy.

B. Prohibited Fee

Any fee that is charged for access, exchange, or use of EHI shall not be based on:

– Whether the requester or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the Actor;

– Sales, profit, revenue, or other value that the requester or other persons derive or may derive from the access, exchange, or use of the EHI;

– Costs the Actor incurred due to Actor having had purposefully designed or implemented its health IT in a non-standard way, unless the requester agrees to the fee associated with the non-standard design or implementation to access, exchange, or use the EHI;

– Costs associated with intangible assets other than the actual development or acquisition costs of such assets;

– Opportunity costs unrelated to the access, exchange, or use of EHI;

and/or

– Any costs that led to the creation of intellectual property, if the Actor charged a royalty for that intellectual property pursuant to § 171.303 and that royalty included the development costs for the creation of the intellectual property.
Act 2

Licensing
Compliance To Do
Info Blocking “To Do” List

- Assemble a “team” to tackle Information Blocking.
  - Legal/Compliance
  - Privacy Officer
  - Vendor/EMR representative
  - IT/Security

- Determine what type(s) of “Actor” is your organization?
  - Health Care Provider
  - HIE/HIN
  - Certified Health IT Vendor

- Identify/evaluate current practices for potential info blocking
  - Patient Portals
  - Provider Portals
  - EMR requests for access; exchange; use of EHI
  - Review HIPAA Business Associate Agreements & update if needed
Info Blocking Compliance: “To Do” List (con’t)

- Develop basic Information Blocking **policies:**
  - Preventing Harm
  - Security
  - Privacy
  - Infeasibility
  - Health IT Performance
  - Fees
  - Content & Manner
  - Licensing

- Implement compliant **practices:**
  - **Preventing Harm**
    - Use a harm “decision tree” for determinations
    - Practitioner training/education
    - Make determinations based on written Organizational Policy or Episodic
  - **Privacy**
    - Review & update Consent process
      - Identify exceptions to consent under applicable federal & state law
      - Process for “reasonable efforts” to facilitate obtaining compliant consent when required
    - Review & update HIPAA Right of Access & Personal Representatives P&Ps
      - Minors & Parents
      - Guardians & other legal representatives
      - Unreviewable denials of access
    - Review & update HIPAA Request for Confidential Communications P&Ps
    - Training as needed for registration, HIM, medical records, staff etc.
    - Make determinations based on written Organizational Policy or Episodic
Info Blocking Compliance: “To Do” List (con’t)

☐ Implement compliant practices:

☐ Infeasibility
  - Use an infeasibility “decision tree” for determinations. Document.
  - Use a “Notice of Infeasibility” to inform requestor when a decision is made to deny access, exchange or use of EHI due to infeasibility.

☐ Content & Manner – determine if only USCDI data will be provided, or all EHI

☐ Identify how requests for EHI are going to received and escalated for Info Blocking evaluation going forward.
**What questions or practical issues would you like to see addressed in the Information Blocking learning sessions from a Compliance and/or IT perspective?**

1. Sharing/blocking psychotherapy notes with patients/parents/guardians. Information Blocking rule vs. HIPAA-preemption analysis. Including when they are part of an integrated health record (i.e., not kept separate from the health record). PRIVACY EXCEPTION

2. Latitude of ability to release information for care coordination purposes to non-covered entity PRIVACY EXCEPTION; PROPOSED CHANGES TO HIPAA PRIVACY RULE

3. Examples of patient data that fall under the self-harm clause. Tips on how to implement policy and how to document PREVENTING HARM EXCEPTION; TIP SHEET

4. Implications for behavioral health providers/SUD and BH compliance issues PRIVACY EXCEPTION; TECHNOLOGY (segmentation)

5. Questions surrounding auto-release of results to patient portals e.g., risk of feeding information to a patient portal before provider review. INFORMATION BLOCKING; PREVENTING HARM; INFEASIBILITY

6. What turnaround time frames do you recommend when the org has 2 or more EMRs? ONC FAQ.

7. Staff still need crystal-clear explanations of why common steps (e.g. requiring patient request) are info blocking. REQUEST IS PRE-REQUISITE. ONC FAQ ON PORTALS.

8. Questions surrounding making available full clinical notes USCDlv2; CONTENT EXCEPTION.

9. How do the functionality of interfaces effect our legal standing. INFEASIBILITY EXCEPTION

10. Sample compliance P&P LEGAL HIE COMPLIANCE LIBRARY
Questions?

Need sample policies & documentation tools to comply with Information Blocking?

Legal HIE compliance library:  www.legalhie.com/membership