



COMMUNITY
HEALTH CARE
ASSOCIATION
of New York State

*CHCANYS NYS-HCCN is partnering
with Attorneys at Oscislawski LLC to
present*

Information Blocking Rule Learning Session 2 Technology Focus

October 28, 2021 – 1:00 pm

Zoom Guidelines

- You have been muted upon entry. Please share your comments or questions in the chat window
- The webinar is being recorded.



**Helen Oscislawski, Esq.,
Founder & Managing Partner
Attorneys at Oscislawski LLC.**



Attorneys at
Oscislawski LLC



Information Blocking

Part 2 – Technical Implementation

October 28, 2021

prepared for

CHCANYS

presented by

Helen Oscislowski, Esq.



Attorneys at
Oscislowski LLC



About Helen O.

Helen was just selected Best Lawyers® **2022 “Lawyer of the Year”** for Health Care Law in Princeton, New 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.

Q&As from Learning Session 1

- Who decides if an App is secure or not? What is it based on?
- Our psychiatrists and psychologists have concerns about patients having access to entire notes. What can you do?
- Can you state that it is infeasible if your EHR vendor has the system set such that a provider has to sign off on results before they can go to the portal and the EHR vendor has yet to resolve this issue despite months of requests?
- If a patient has not signed up for the patient portal, we would continue to follow straight HIPAA law unless they ask for their records in some electronic format, correct?
- In the event an EHR system offers record sharing accounts (i.e., parents with minors) and the system is setup such that all records or no records are shared, what considerations do the health centers need to be thinking about and to include in writing their policies should they choose to turn off this feature when it comes to sharing lab results, clinical notes, etc. Is this putting health centers at risk for blocking information?
- Is a ransomware lockdown considered an 'uncontrollable event'?
- How about drug and alcohol use as described in Social History? it looks like yes (that should be shared) based on this document.



New Questions

- **MINORS RECORDS!**
 - Access to Minor Records and Custodial issues with children and adults
 - Would like to learn more about minors
 - Ways to share medical info with adolescents, what is the minimum requirement if info sharing required for patients to meet rule
- Would like to discuss any **applicability of Cures Act** to patients **not accessing records digitally**.
- **Email encryption** - both Health Information and business information

“Actors”

3 Categories of Actors

“Health Care Providers”

***“Health Information Networks” and
“Health Information Exchanges”***

“Developers of Certified Health IT”

Health Information Networks and Health Information Exchanges

An individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for *access, exchange, or use of EHI*:

- Among *more than two* “unaffiliated” individuals or entities that are enabled to exchange EHI with each other;

and

- For treatment, payment, or health care operations

Are you operating as a HIE/HIN?



Health IT Developer of Certified Health IT

An individual or entity

-- other than a health care provider that self-develops health IT for its own use –

- That ***develops*** or ***offers*** health information technology
 - **and**
- Has *one or more Health IT Modules* **certified** under a program for the ***voluntary certification*** by ONC's Health HIT Certification Program

Are you offering certified Health IT?

TO DO

- ☐ Determine if your organization engages in any activities that might fit the definition of "**Health Information Network (HIN) or Health Information Exchange (HIE)**"
- ☐ Determine if your organization engages in any activities that might fit the definition of offering "**Certified Health IT**"

“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*)



Example #1: “*Interferes With*”

An EHR developer of certified health IT requires third-party applications to be “***vetted***” for security before use but does not promptly conduct the vetting or *conducts the vetting in a discriminatory or exclusionary manner.*

Example #2: “*Interferes With*”

An HIE/HIN or Health IT Vendor charges *additional fees*, requires *more stringent testing* or certification requirements, or imposes *additional terms* for *participants that are competitors*, are *potential competitors*, or may use EHI obtained via the HIN in a way that facilitates competition with the HIN.

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, the *functionality is purposefully not enabled*.



Example #4: *Delaying Access*

An EMR is capable of providing *same-day access to EHI* (e.g., lab results) 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 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?* (IB.FAQ24.1.2021JAN)

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

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 (85 FR 25813).
- 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 (see also 85 FR 25813).
- 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 ...

ONC FAQ:

Blanket Delays likely Interference

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.

www.healthit.gov/curesrule/faq/when-would-delay-fulfilling-request-for-access-exchange-or-use-ehi-be-considered-interference



ONC FAQ:

Proactive Push Not Required

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? (IB.FAQ23.1.2021JAN)

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 (85 FR 25813, 25878). If the delay were to constitute an interference under the information blocking regulations, an actor’s practice or actions may still satisfy the conditions of an exception under the information blocking regulations (45 CFR 171.200-303).

www.healthit.gov/curesrule/faq/do-information-blocking-regulations-45-cfr-part-171-require-actors-proactively-make-electronic

TO DO

Identify technical practices that "*interfere with*" (e.g., delay; block; discourage) access, exchange and use of EHI. Review the following:

- Patient Portal
- Provider Portal
- EMR – *requests for:*
 - Access
 - Exchange
 - Use

8 Safe Harbors

1.Preventing Harm

2.Privacy

3.Security

4.Infeasibility

5.Health IT Performance

6.Fees

7.Licensing

8.Content & Matter

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.



Implementation

☐ **Organizational policy:**

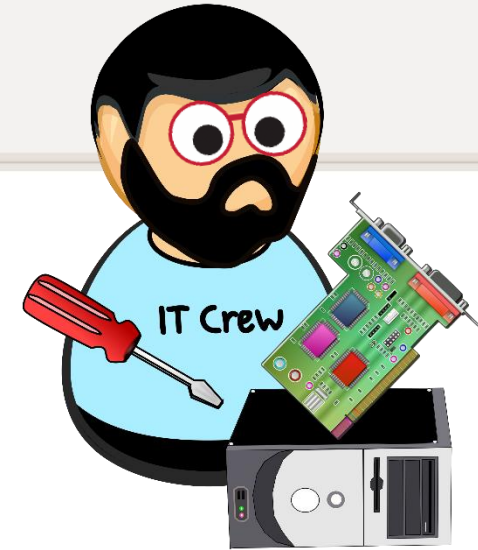
- ✓ Be in writing
- ✓ Be based on relevant clinical, technical, and other appropriate expertise;
- ✓ Be implemented in a consistent and non-discriminatory manner; and
- ✓ Conforms each practice to the conditions in paragraphs (a) and (b) of this section, as well as the conditions in paragraphs (c) through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

OR

☐ **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.

Technical Implementation



- ❑ Capturing the health care professional's determination
 - EMR field
 - Clinical Notes
 - Look to HIPAA
 - *How is it done when access rights are denied per HIPAA?*
 - *How is the determination communicated for IT implementation?*
- ❑ How can the EHI be “blocked”?
 - Granularity (e.g., per episode; per type of data)
 - All-or-nothing

Privacy Exception

Four (4) 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 their EHI

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, certain federal and state laws require *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

❑ PNS: Documentation Requirement

- ❑ 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.

Technical Implementation

- ❑ Identify applicable privacy laws
- ❑ How does the EHI restricted?
 - General consent
 - Specific consent
 - Notice
 - Other condition
- ❑ How can the EHI be “blocked”?
 - Granularity
 - Provider type – e.g., mental health unit)
 - Patient type – e.g., emancipated minor
 - Data type – e.g., HIV/AIDS
 - All-or-nothing



3. Denial of Right of Access (HIPAA)

If an individual requests EHI under the **right of access** provision under 45 CFR 164.524(a)(1), the Actor's 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

Technical Implementation



- ❑ Capture the Reason for Denial of Access
 - Field in EMR
 - Notes
 - Look to HIPAA
 - *How is it done when access rights are denied per HIPAA?*
 - *How is a patient/PR permitted to request restrictions?*
 - *How is the determination communicated for IT implementation?*

- ❑ How can the EHI be “blocked”?
 - Granularity (e.g., per date? per data type (e.g., research))
 - All-or-nothing

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.

Technical Implementation



- ❑ Capture the requested restriction
 - EMR field
 - Notes
 - Look to HIPAA
 - *How is a patient/PR permitted to request restrictions?*
 - *How is the determination communicated for IT implementation?*
- ❑ Can the EHI be “blocked” as requested?
 - Granularity
 - All-or-nothing

Security Exception

Elements of the Exception

The practice **must** be:

- ❑ **Directly related to safeguarding** the confidentiality, integrity, and availability of EHI;
- ❑ **Tailored** to specific security risks; and
- ❑ Implemented in a **consistent** and ***non-discriminatory*** manner.

Conditions

-EITHER-

Make a **Determination** *in each case*, based on the particularized facts and circumstances that:

1. Practice is ***necessary*** to **mitigate** *the security risk* to EHI;
and
2. **No reasonable & appropriate alternatives** to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.

-OR-



Conditions (*con't*)

Implement the practice through an **Organizational Security Policy** (“OSP”) that:

1. Is in writing
2. Is prepared on the basis of, and be **directly responsive to**, the ***security risks*** **identified** and assessed by or on behalf of Actor;
3. Align with one or more applicable ***consensus-based standards*** or ***best practice guidance***; and
4. Provide ***objective timeframes*** and other parameters for identifying, responding to, and addressing security incidents.

OSP: *Identify Security Risks*

- HIPAA Security Risk Analysis
- *Other* Risk Assessments:

*A good risk assessment uses an approach
consistent with industry standards, and
incorporates elements such as:*

- *threat and vulnerability analysis*
- *data collection*
- *assessment of current security measures*
- *likelihood of occurrence*
- *impact*
- *level of risk*
- *final reporting*

OSP: *Implementing Security Practices*

1. Tailored to the **specific** Security Risk
2. Consistent and Non-Discriminatory
3. Consensus-Based or Best Practice Guidance
 - **NIST-800-53 Rev. 5**;
 - **NIST Cybersecurity Framework**; and
 - NIST **SP 800-100**, **SP 800-37 Rev. 2**, **SP 800-39**, as updated and as interpreted through formal guidance.
 - Examples of best practice guidance on security policies developed by consensus standards include: **ISO**, **IETF**, or **IEC**.

OSP: *Implementing Security Practices*

1. Tailored to the **specific** Security Risk
2. Consistent and Non-Discriminatory
3. Consensus-Based or Best Practice Guidance
 - **NIST-800-53 Rev. 5**;
 - **NIST Cybersecurity Framework**; and
 - NIST **SP 800-100**, **SP 800-37 Rev. 2**, **SP 800-39**, as updated and as interpreted through formal guidance.
 - Examples of best practice guidance on security policies developed by consensus standards include: **ISO**, **IETF**, or **IEC**.

<p>NIST Special Publication 800-37, Revision 2</p> <p>Security and Privacy Information Systems and Organizations</p> <p>This publication is available at https://doi.org/10.26206/1.29172</p>	<h3>3.16 RISK ASSESSMENT</h3> <p>Quick link to Risk Assessment Summary Table</p> <h4>RA-1 POLICY AND PROCEDURES</h4> <p><u>Control:</u></p> <ul style="list-style-type: none"> a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: <ul style="list-style-type: none"> 1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that: <ul style="list-style-type: none"> (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: <ul style="list-style-type: none"> 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]. <p><u>Discussion:</u> Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.</p> <p><u>Related Controls:</u> PM-9, PS-8, SI-12.</p> <p><u>Control Enhancements:</u> None.</p> <p><u>References:</u> [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].</p>	<p>PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS</p> <p>Contents</p> <ul style="list-style-type: none"> 1 2 3 3 5 5 6 7 7 8 11 13 14 16 18 59 65 83 96 115 131 149 162 171 179 194 203 222 229 238 249 292 332 363 374 394 424 427
--	---	---

OSP: *Timeframes for Identifying, Responding to, and Addressing Security Risks*

1. OSP must include a Security Response Plan that provides **objective timeframes** and **common terminology** used for identifying, responding to, and addressing security incidents.
2. Acceptable sources for development of a Security Response Plan include:
 - NIST Incident Response Procedure [SP 800-61, Rev. 2](#);
 - US-CERT for interactions with government systems (<https://www.uscert.gov/government-users/reportingrequirements>); and
 - ISC-CERT for critical infrastructure (<https://icscert.us-cert.gov/>) (84 FR 7537).

OSP: *Timeframes for Identifying, Responding to, and Addressing Security Risks*

1. OSP must include a Security Response Plan that provides **objective timeframes** and **common terminology** used for identifying, responding to, and addressing security incidents.
2. Acceptable sources for development of a Security Response Plan include:
 - NIST Incident Response Procedure [SP 800-61, Rev. 2](#);
 - US-CERT for interactions with government systems (<https://www.uscert.gov/government-users/reportingrequirements>); and
 - ISC-CERT for critical infrastructure (<https://icscert.us-cert.gov/>) (84 FR 7537).

OSP: Timeframes for Identifying, Responding to, and Addressing Security Risks

<p>NIST Special Publication 800-61 Revision 2</p> <p>Computer Security Incident Handling Guide</p> <p><i>Recommendations of the National Institute of Standards and Technology</i></p> <p>COMPUTER</p> <p>U.S. Department of Commerce Rebecca Blank, Acting Secretary</p> <p>National Institute of Standards and Technology Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director</p>	<p>COMPUTER SECURITY INCIDENT HANDLING GUIDE</p> <p>Table of Contents</p> <p>Executive Summary 1</p> <p>1. Introduction 4</p> <p>..... 4</p> <p>..... 4</p> <p>..... 4</p> <p>..... 4</p> <p>..... 6</p> <p>..... 6</p> <p>..... 6</p> <p>..... 7</p> <p>..... 7</p> <p>..... 8</p> <p>..... 8</p> <p>..... 9</p> <p>..... 13</p> <p>..... 13</p> <p>..... 14</p> <p>..... 16</p> <p>..... 17</p> <p>..... 18</p> <p>..... 19</p> <p>..... 21</p> <p>..... 21</p> <p>..... 21</p> <p>..... 23</p> <p>..... 25</p> <p>..... 25</p> <p>..... 26</p> <p>..... 27</p> <p>..... 28</p> <p>..... 30</p> <p>..... 32</p> <p>..... 33</p> <p>..... 35</p> <p>..... 35</p> <p>3.3.1 Choosing a Containment Strategy 36</p> <p>3.3.2 Evidence Gathering and Handling 36</p> <p>3.3.3 Identifying the Attacking Hosts 37</p> <p>3.3.4 Eradication and Recovery 37</p> <p>3.4 Post-Incident Activity 38</p> <p>3.4.1 Lessons Learned 38</p> <p>3.4.2 Using Collected Incident Data 39</p> <p>3.4.3 Evidence Retention 41</p> <p>3.5 Incident Handling Checklist 42</p> <p>3.6 Recommendations 42</p> <p>4. Coordination and Information Sharing 45</p>
---	---

What About Risks Not addressed by OSP?

- **That's OK.** Make “determination” based on particularized facts and circumstances that Security Practice is *necessary* to *mitigate security risk* and *no reasonable* and *appropriate alternatives* to the Security Practice that address the security risk and are less likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.
- *Exigent/Emergency Circumstance?*
 - Delay for assessment not expected. May implement emergency Security Practice in *good faith*
 - Intended only for **short time**. *Expeditionously* make any necessary changes – replace with “reasonable & appropriate” alternative measures that are less likely to interfere with access, exchange, or use of EHI as expeditiously as possible.

Documentation

“Many of these conditions are related to other existing regulatory requirements that have similar documentation standards. For example, an actor’s practice may meet the Security Exception at § 171.203 if it is consistent with an organizational security policy and that policy meets several requirements. ***We expect that many actors have existing organizational security policies based on the “Policy and procedures and documentation requirements” in the HIPAA Security Rule at 45 CFR 164.316.*** Consequently, the burden associated with meeting the documentation requirement in the Security Exception should be less if actors are already complying with the HIPAA Security Rule.”



Framework Security Policy

Legal Health information eXchange™

POLICY: Security Exception

CATEGORY: Information Blocking

POLICY TOPIC: Security Exception

EFFECTIVE DATE: April 5, 2021

I. POLICY

Provider 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* Provider is required by law to do so, or Provider must Block EHI in order to protect the security of electronic health information (EHI). If Provider decides to Block EHI in order to protect the security of EHI, it shall do so only if such Practice is: (i) directly related to safeguarding the confidentiality, integrity, and availability of EHI; (ii) tailored to the specific security risk being addressed; and (iii) implemented in a consistent and non-discriminatory manner.

A Practice that is aimed at protecting the security of EHI but is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI will be implemented in accordance with Provider's "*Organizational Security Policy*," or otherwise determined in each case in accordance with this Policy.

II. PROCEDURE

A. Organizational Security Policy

(1) Provider shall maintain an *Organizational Security Policy* that is prepared on the basis of, and be directly responsive to, security risks identified and assessed by Provider, or which have been identified and assessed by a vendor on behalf of Provider.

(2) In exigent circumstances where Provider must implement a Practice to respond to a security risk that has not been identified in Provider's *Organizational Security Policy*, Provider may proceed in accordance with "Section E." below.

B. Identifying Security Risks

(1) In accordance with 45 CFR 164.308(a)(1)(ii)(A) of the HIPAA Security Rule and Provider's applicable HIPAA Security policies, Provider shall conduct an accurate and thorough assessment (a "HIPAA Risk Analysis") of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by Provider. Potential security risks and vulnerabilities identified in such HIPAA Risk Analysis shall be documented, and must be used as a basis upon which Provider will determine which security practices to implement in order to safeguard the confidentiality, integrity, and availability of EHI.

© 2021 Legal HIE Solutions LLC. All rights reserved.
DISCLAIMER: Do not rely on this sample to make any decision which requires the advice of an attorney.

Legal Health information eXchange™

POLICY: Security Exception

(2) Provider may conduct additional security risk assessments as specified and in accordance with Provider's *Organizational Security Policy*. Provider recognizes that a good risk assessment uses an approach consistent with industry standards, and incorporates elements such as threat and vulnerability analysis, data collection, assessment of current security measures, likelihood of occurrence, impact, level of risk, and final reporting. Any such additional security risk assessments completed shall be documented, and must be used as a basis upon which Provider will determine which security practices to implement in order to safeguard the confidentiality, integrity, and availability of EHI.

C. Implementing Security Practices. All of the following conditions (1)-(4) shall be addressed in Provider's *Organizational Security Policy*:

(1) ***Tailored to the Specific Security Risk.***

a. Any and all security Practices Provider implements in response to security risks must be *tailored to the specific risks identified* in its HIPAA Risk Analysis and/or other security risk assessment.

b. Any security Practice that Provider has implemented or intends to implement consistent with a *minimum* legal condition related to the security of EHI (e.g., in accordance with law or policy) shall be evaluated to determine if such Practice might not meet this Security Exception if it is not also *tailored* to avoid interfering with the access, exchange, or use of EHI to a greater extent than reasonable and necessary to appropriately mitigate the risk it addresses.

(2) ***Consistent and Non-Discriminatory.***

a. If Provider requires certain tailored security requirements be met, those security requirements shall be imposed in a non-discriminatory manner. This means, for example, that if Provider imposes a requirement that a third-party include *two-factor authentication* for patient access, Provider shall ensure that the same requirement is imposed on, and met by, all other third-parties.

b. Practices applied on the basis of the cybersecurity risks posed by particular system connections or data exchanges may result in Practices that are tailored to this risk and thus not necessarily identical across all connections, interchanges, and therefore all individuals or entities with whom Provider engages.

c. In context of this condition of this Security Exception policy, "consistent and non-discriminatory" shall mean that similarly situated individuals or entities whose interactions pose the same level of security risk should be treated consistently with one another under their respective security practices. Inconsistent treatment across similarly situated Actors whose interactions pose the same level of security risk based on extraneous factors, such as whether they are a competitor of the Actor implementing the security practices, would not be considered appropriate.

© 2021 Legal HIE Solutions LLC. All rights reserved.
DISCLAIMER: Do not rely on this sample to make any decision which requires the advice of an attorney.



TO DO

- ☒ Develop a Security Exception policy (see sample)
- ☐ Review/develop a written **Organizational Security Policy** (OSP) that:
 - Identifies specific security **risks** (HIPAA risk assessment; industry standards)
 - Reflects **practices** tailored to the identified risks that are consensus-based or industry best practices
 - Includes a **security response plan** for incidents & new risks
- ☐ Implement security practices in a **consistent** and **non-discriminatory** manner
- ☐ Evaluate & address new security risks as they come up or in response to new requests for EHI

Infeasibility Exception

“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.

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.

“One-Off” Interface Requests

Comments. A few commenters encouraged ONC to add a provision to the exception that would enable entities who have joined TEFCA to claim the Infeasibility Exception if a requestor or third party refused to join the TEFCA and instead demanded a one-off interface .

Response. We appreciate these comments, but have decided not to adopt this suggested addition at this time. The TEFCA is still new, the Common Agreement is not yet finalized, and it would be premature to establish special treatment for entities that join the TEFCA. We may reconsider this suggestion at a later date. We note that ***this does not necessarily mean that actors in these situations will not be covered by the exception, as they could still show that a request for a one-off interface is infeasible under the circumstances*** (see § 171.204(a)(3)). However, not joining TEFCA is not de facto proof of infeasibility. We note that in addition to seeking coverage for infeasibility under the circumstances, **the actor could also seek coverage from: (1) The Content and Manner Exception if the actor could not fulfill request to access, exchange, or use EHI in the manner requested (via a one-off interface), but could fulfill the request through an acceptable alternative manner (see § 171.301(b)); or (2) the Fees Exception or Licensing Exception if the actor chooses to provide the one-off interface as requested, but charges fees/royalties related to developing or licensing the one-off interface, which could include fees or royalties that result in a reasonable profit margin (see § 171.302 and 303)**

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

Legal Health information exchange

FORM: Notice of Infeasibility

NOTICE OF INFEASIBILITY
(pursuant to 45 CFR 171.204(b))

Date 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 FULFILLING THE REQUEST FOR THE FOLLOWING REASON(S) (see "checked" 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 ePHI 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 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 [Actor]'s right to deny access rights under HIPAA.

☐ Requestor asking for *more than USCDI data* (before May 2, 2022), and Actor is 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 use 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.

© 2020 Legal IHE Solutions LLC. All rights reserved.
DISCLAIMER: This tool is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts. Do not rely on this tool to make any decision which requires the advice of an attorney.
This information was last updated October 2020.



Infeasibility Exception Decision Tree

Legal Health information exchange[®]

FORM: Infeasibility Under the Circumstances

Uncontrollable Event: Is there an *uncontrollable event* that makes it *infeasible* to fulfill the request?

☐ YES **STOP.** Actor may claim Infeasibility Exception & Block EHI for duration of the event]

☐ NO *(continue)*

Segmentation: Is it technologically *infeasible* to *unambiguously segment* the EHI requested from other ePHI 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 Actor has honored this;

☐ Federal or state *law prohibits* it from being disclosed; or

☐ There would be “*substantial harm*” to the individual or another person if request is fulfilled in manner requested (follow Preventing Harm Exception requirements/analysis)?

☐ YES - **STOP.** See Infeasibility Exception; Privacy Exception; Preventing Harm Exception.

☐ NO *(continue)*

Infeasibility Under the Circumstances:

A. Document the Infeasibility Factors (REQUIRED):

1. Type of EHI Requested: _____

2. Purpose(s) for which EHI is requested/needed: _____

3. Cost to the Actor of complying 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 EHI to its own companies, or to customers, suppliers, partners, and other persons with whom it has a business relationship?

☐ No ☐ Yes If yes, explain why the circumstance is different here: _____

6. Does Actor own or control the predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged?

☐ No ☐ Yes If yes, explain why that control does not allow Actor to readily provide EHI: _____

© 2020 Legal HIE Solutions LLC. All rights reserved.
DISCLAIMER: This tool is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts.
Do not rely on this tool to make any decision which requires the advice of an attorney.
This information was last updated October 2020.

1

Legal Health information exchange[®]

FORM: Infeasibility Under the Circumstances

B. Is it feasible to fulfill the request for EHI *in manner asked*?

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** USCDI data (before May 2, 2022), can Actor:

☐ Provide requestor with **all** EHI requested?

☐ YES - **STOP.** Provide requestor with EHI data requested.

☐ NO *(continue)*

☐ Segment USCDI data from other EHI, and only release USCDI data?

☐ YES - **STOP.** Provide requestor with USCDI data.

☐ NO *(continue)*

C. Is feasible to fulfill the request for EHI in an *alternative manner*?

1. Can Actor use 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 requestor to furnish the USCDI/EHI data requested?

☐ YES - **STOP.** Provide requestor with USCDI/EHI data in the alternative manner.

☐ NO *(continue)*

© 2020 Legal HIE Solutions LLC. All rights reserved.
DISCLAIMER: This tool is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts.
Do not rely on this tool to make any decision which requires the advice of an attorney.
This information was last updated October 2020.

2

Legal Health information exchange[®]

FORM: Infeasibility Under the Circumstances

2. Can Actor use content and transport standards specified by requestor and published by: the federal government, or a standards-developing organization accredited by the American National Standards Institute (ANSI) to furnish the USCDI/EHI data requested?

☐ YES - **STOP.** Provide requestor with USCDI/EHI data in the alternative manner.

☐ NO *(continue)*

3. Can Actor use an alternative machine-readable format, including the means to interpret the EHI, agreed upon with requestor to furnish the USCDI/EHI data requested?

☐ YES - **STOP.** Provide requestor with USCDI/EHI data in the alternative manner.

☐ NO - **STOP.** Actor may assert Infeasibility Exception based on “**Infeasibility Under the Circumstances.**”

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

© 2020 Legal HIE Solutions LLC. All rights reserved.
DISCLAIMER: This tool is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts.
Do not rely on this tool to make any decision which requires the advice of an attorney.
This information was last updated October 2020.

3

TO DO

- ☐ Develop a Infeasibility Exception **policy**.
- ☐ Use a **decision tree** tool to evaluate new EHI requests under the Infeasibility Exception.
- ☐ Use a "**Notice of Infeasibility**" to inform requestor when a decision is made to deny access, exchange or use of EHI due to infeasibility. Ensure that decisions are **consistent** and do **not discriminate**.

Health IT Performance

Must Meet *at Least One* of the Following Conditions:

- Maintenance & Improvements
- Assured level of performance
- Practices that Prevent Harm
- Security-related Practices



Maintenance & Improvements

Actor's practice must be—

(1) Implemented for a *period of time no longer than necessary* to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded; and

(2) Implemented in a *consistent* and *non-discriminatory* manner.

Maintenance & Improvements

IF the unavailability or degradation is initiated by a health IT developer of certified Health IT or HIE/HIN:

- *Planned:* Must be **consistent** with existing **service level agreements** between the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT;

or

- *Unplanned:* Must be **consistent** with existing **service level agreements** between the individual or entity; **or agreed to** by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

Assured Level of Performance

Actor may take **action against a third-party application** that is negatively impacting the health IT's performance, provided that the practice is—

- For a period of time *no longer than necessary* to resolve any negative impacts;
- Implemented in a *consistent* and *non-discriminatory* manner; and
- Consistent with existing *service level agreements*, where applicable

Harm & Security Practices

Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by Actor in response to a risk of harm to a patient or another person, Actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by Actor in response to a security risk to EHI, Actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

TO DO

- ❑ Develop a Health IT Exception **policy**.
- ❑ Evaluate new EHI requests under the Health IT Exception as appropriate.
- ❑ Ensure that decisions to delay or deny access, exchange and use of EHI are:
 - For **no longer than necessary**
 - **Consistent** and do **not discriminate**

Fees Exception

Elements of the Fees 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)***;
- (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.

Content & Manner

Content

- 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)

USCDI Standard v.2 (July 2021)

Visit: [United States Core Data for Interoperability \(USCDI\) - July 2021 - Version 2 \(healthit.gov\)](https://www.healthit.gov/data/uscdi)

The USCDI v2 contains data classes and elements from USCDI v1 and new data classes and elements submitted through the ONDC system. Please reference the [USCDI Version 2 document](#) to the left for applicable vocabulary standards versions associated with USCDI v2 and to the [ONC Standards Bulletin 21-3](#) for more information about the process to develop USCDI v2 and future versions.

Allergies and Intolerances

Represents harmful or undesirable physiological response associated with exposure to a substance.

Reaction
Substance (Drug Class)
Substance (Medication)

Goals

An expressed desired health state to be achieved by a subject of care (or family/group) over a period of time or at a specific point of time

Patient Goals
SDOH Goals

Problems

Information about a condition, diagnosis, or other event, situation, issue, or clinical concept that is documented.

Date of Diagnosis
Date of Resolution
Problems
SDOH Problems/Health Concerns

Assessment and Plan of Treatment

Represents a health professional's conclusions and working assumptions that will guide treatment of the patient.

Assessment and Plan of Treatment
SDOH Assessment

Health Concerns

Health related matter that is of interest, importance, or worry to someone who may be the patient, patient's family or patient's health care provider.

Health Concerns

Procedures

An activity that is performed with or on a patient as part of the provision of care.

Procedures
SDOH Interventions

Care Team Member(s)

The specific person(s) who participate or are expected to participate in the care team.

Care Team Member Identifier
Care Team Member Location
Care Team Member Name
Care Team Member Role
Care Team Member Telecom

Immunizations

Record of an administration of a vaccination or a record of a vaccination as reported by a patient, a clinician, or another party.

Immunizations

Provenance

The metadata, or extra information about data, that can help answer questions such as when and who created the data.

Author Organization
Author Time Stamp

Clinical Notes

Represents narrative patient data relevant to the respective note types.

Consultation Note
Discharge Summary Note
History & Physical
Procedure Note
Progress Note

Laboratory

Tests
Values/Results

Smoking Status

Representing a patient's smoking behavior.

Smoking Status

Clinical Tests

Includes non-imaging and non-laboratory tests performed on a patient that results in structured or unstructured (narrative) findings specific to the patient, such as electrocardiogram (ECG), visual acuity exam, macular exam, or graded exercise testing (GXT), to facilitate the diagnosis and management of conditions.

Clinical Test Result/Report
Clinical Test

Medications

Medications

Unique Device Identifier(s) for a Patient's Implantable Device(s)

A unique numeric or alphanumeric code that consists of a device identifier (DI) and a production identifier (PI).
Unique Device Identifier(s) for a patient's implantable device(s)

Diagnostic Imaging

Tests that result in visual images requiring interpretation by a credentialed professional.

Diagnostic Imaging Report
Diagnostic Imaging Test

Patient Demographics

Current Address
Date of Birth
Email Address
Ethnicity
First Name
Gender Identity
Last Name
Middle Name (including middle initial)
Phone Number
Phone Number Type
Preferred Language
Previous Address
Previous Name
Race
Sex (Assigned at Birth)
Sexual Orientation
Suffix

Vital Signs

Physiologic measurements of a patient that indicate the status of the body's life sustaining functions.

BMI Percentile (2 - 20 years)
Body height
Body temperature
Body weight
Diastolic blood pressure
Head Occipital-frontal Circumference Percentile (Birth - 36 Months)
Heart Rate
Inhaled oxygen concentration
Pulse oximetry
Respiratory rate
Systolic blood pressure
Weight-for-length Percentile (Birth - 36 Months)

Encounter Information

An episode defined by an interaction between a healthcare provider and the subject of care in which healthcare-related activities take place.

Encounter Diagnosis
Encounter Disposition
Encounter Location
Encounter Time
Encounter Type

Technical Implementation

- ☐ Identify EMR Fields that are USCDI.
- ☐ Can USCDI be **segmented** from all other EHI?
 - ☐ **Yes.** *May* (for purposes of IBR) block non-USCDI data, but must provide USCDI through October 5, 2022.
 - ☐ **No.** Can assert Infeasibility Exception. No EHI must be provided for purpose of IBR compliance.



Manner Condition

- ❑ Actor **must** fulfill a request *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.
- ❑ If Actor fulfills a request *in any manner* requested:
 - **Any fees charged by Actor** in relation to fulfilling the response are **not** required to satisfy the exception in § 171.302 (Fees Exception);

and
 - 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

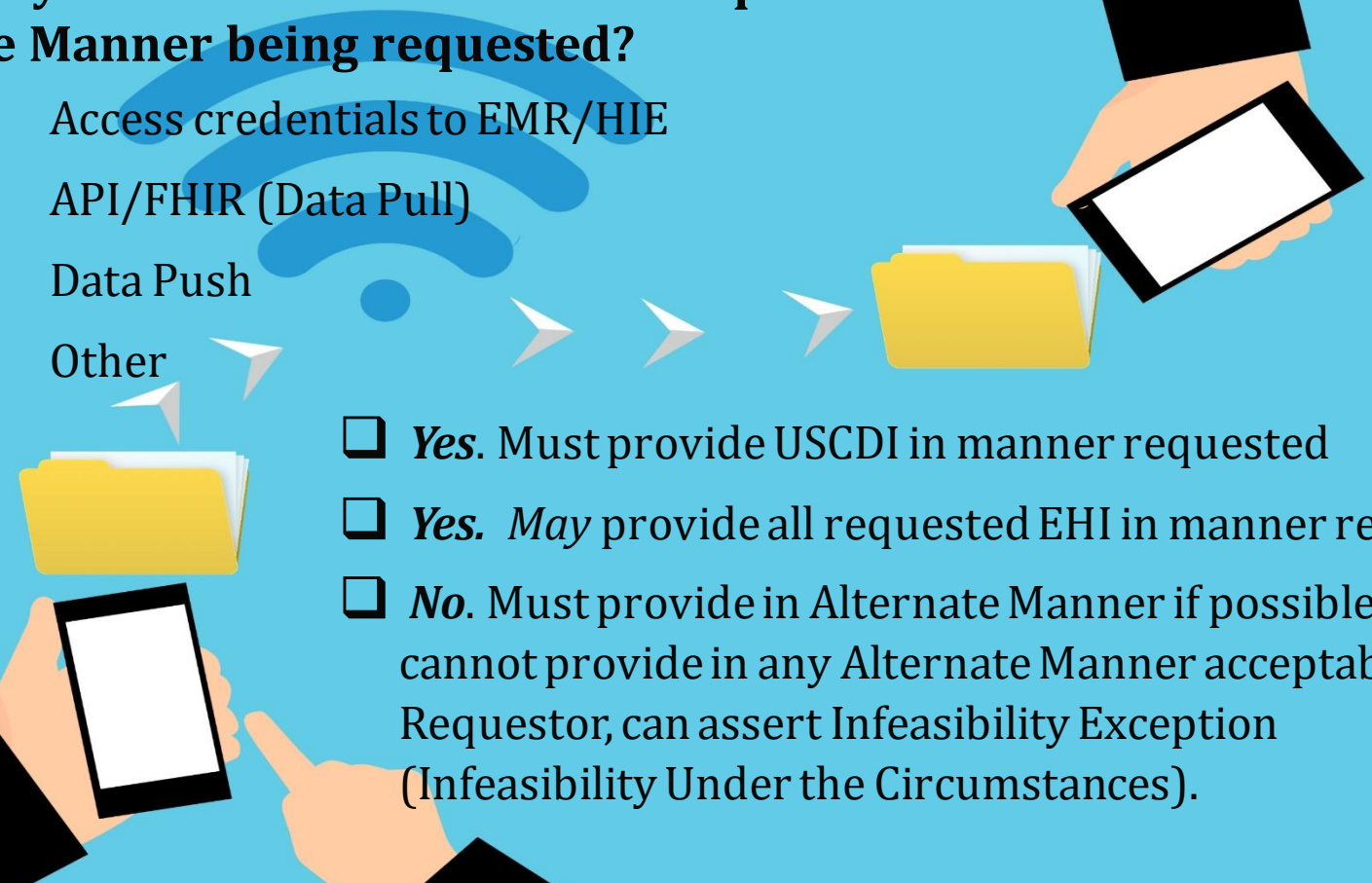
- ❑ Actor must fulfill the request *without unnecessary delay* in the following order of priority, starting with first and only proceeding to the next consecutive alternative if Actor is technically unable to fulfill the request in the manner identified in a paragraph:
 - Using technology certified to 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.
- ❑ Any **fees** charged by Actor in relation to fulfilling the request are required to *satisfy the exception* in § 171.302 (Fees Exception).
- ❑ Any **license** of interoperability elements granted by Actor in relation to fulfilling the request is required to satisfy the exception in § 171.303 (Licensing Exception).



Technical Implementation

☐ Can you make EHI available to Requestor in the Manner being requested?

- Access credentials to EMR/HIE
- API/FHIR (Data Pull)
- Data Push
- Other

- 
- ☐ **Yes.** Must provide USCDI in manner requested
 - ☐ **Yes.** *May* provide all requested EHI in manner requested
 - ☐ **No.** Must provide in Alternate Manner if possible. If cannot provide in any Alternate Manner acceptable to Requestor, can assert Infeasibility Exception (Infeasibility Under the Circumstances).

Minor's Records & Patient Portals

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.¹ 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 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 provider, 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 belief that (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.²

¹ 45 CFR 164.502(g)(3)(i).

² 45 CFR 164.502(g)(5). HIPAA expressly allows the covered to make this decision notwithstanding a State law . . . to the contrary — *Id.*

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 §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 §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 where 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 §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 § 164.524 to, protected health information about an unemancipated minor to a parent and/or legal guardian . . .".³ 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.⁴

- For purposes of Part 2, a "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

³ 45 CFR 164.502(g)(3)(i)(B) (emphasis added).

⁴ Note, there is a Proposed Rule to change this requirement to 42 C.F.R. Part 2 that, if adopted "as is" in the final rule will apply HIPAA's standards to re-disclosures of Part 2 records received by an entity that is not directly covered by 42 C.F.R. Part 2.



Technical Implementation

- ❑ Which categories of care can a minor assert rights independent of the parent under New York law? (e.g., pregnancy? STD testing? HIV/AIDS? mental health? substance abuse?)
- ❑ Can the EMR technology support managing ***separate portals*** for the parent/minor (with consent of the parent)?
- ❑ Can the EMR technology support ***segmenting & preventing*** certain ***episodes of care*** or ***data*** from being pushed to the patient portal?
- ❑ If the EMR technology cannot be configured to support protecting a minor's privacy rights under state law, then the patient portal may be disabled for minors at a "cut-off" age (e.g., 14) based on state law. If technologically feasible, can still push selected data to the portal (e.g., vaccinations).
 - ➡ *Assert: Privacy Exception & Infeasibility Exception.*



Questions?

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

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



Attorneys at
Oscislawski LLC

Helen Oscislawski, Esq.
Principal, Attorneys at Oscislawski LLC
helen@oscislaw.com
609-835-0833





Announcements

- 6 HIE Compliance Library accounts still available!
- Interoperability Workshop December 7th & 8th – invitation coming soon
- Upcoming Pivotpoint Information Blocking learning sessions



What's Next

NEW educational series: **Empowering Patients Through Information Sharing: Cures Act Compliance**

- Complement and build on existing resources via monthly webinar presentations followed by interactive “Ask the Experts” Q&A sessions
 - November – **Cures Act Overview**
 - Webinar presentation – Wednesday, November 10th, from 12:00-1:00pm
 - Follow-up Ask the Experts Q&A session – Wednesday, Nov 17th, 12:00-1:00pm
 - [REGISTER HERE](#)
 - December – **OpenNotes Overview**
 - Webinar presentation – Wednesday, December 1st, 12:00-1:00pm
 - Follow-up Ask the Experts Q&A session – Wednesday, December 15th, 12:00-1:00pm
 - [REGISTER HERE](#)



Visit the CHCANYS Website for a Full List of Information Blocking Resources and Related Events!



Scan the QR Code to go to the CHCANYS Website

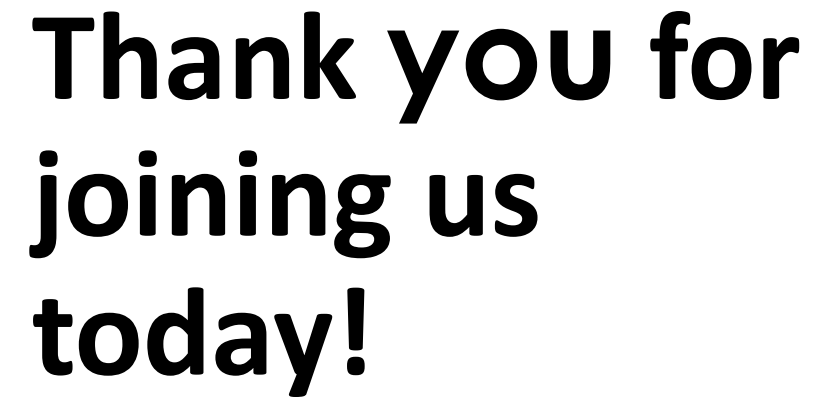


<https://www.chcanys.org/health-center-resources/clinical-technology-resources/health-it/cures-act-information-blocking>



Please share your feedback using the survey link in the chat, the QR code below, or the link in the follow up email!





Contact us: hccn@chcanys.org