healthcurrent

HEALTH CARE PROVIDER TEMPLATE: This is a template policy for health care providers, such as hospitals and physician groups. It is not intended for use by other actors that are subject to the Information Blocking Rule, including health care providers who might also constitute a health information exchange, health information network or health IT developer of certified health information technology.

DISCLAIMER: Every organization is unique. This document is designed to be an educational template, which will need to be tailored to each organization's unique circumstances. The hallmark of an effective policy and compliance program is one that your organization can and does actually implement.

No Information Blocking Policy

PURPOSE

The purpose of this policy is to support Organization's commitment to facilitating the timely Access, Exchange and Use of Electronic Health Information (EHI) in compliance with Applicable Law. Organization will implement this policy in a consistent and non-discriminatory manner.

APPLICABILITY

This policy applies to Organization's workforce members, including employees, officers, medical staff, residents, fellows, students, volunteers, trainees, affiliates, vendors, contractors, consultants, and agents (collectively, "Workforce Members").

Organization's Privacy Official has general responsibility for implementation of Organization's policies and procedures relating to health information, including this No Information Blocking Policy.

NO INFORMATION BLOCKING POLICY

Organization and its Workforce Members will comply with Organization's health information policies and procedures and all Applicable Law in connection with the Access, Exchange or Use of EHI, including this No Information Blocking Policy and the Information Blocking Rule.

The Information Blocking Rule prohibits Actors—including Organization and its Workforce Members—from engaging in practices (such as acts and omissions) that are likely to interfere with the Access, Exchange or Use of EHI, unless the practice is Required by Law or covered by a regulatory exception (collectively, "Safe Harbors"). **The Information Blocking Rule does not require Organization to disclose EHI if doing so would violate other Applicable Law, such as HIPAA or other state or federal privacy laws applicable to Organization.**

The Information Blocking Rule is intent based. That means failure to satisfy a Safe Harbor does not mean that there is a violation of the Information Blocking Rule. However, Organization strives to satisfy the conditions of any applicable Safe Harbor when engaging in practices that might implicate the Information Blocking Rule. Accordingly, Workforce Members will follow this policy and all relevant procedures when engaging in practices that involve the Access, Exchange or Use of EHI over which Organization has control.

KEY DEFINITIONS

Access means the ability or means necessary to make electronic health information available for Exchange or Use.

Actor means a health care provider (as defined in 42 U.S.C. § 300jj), a health IT developer of certified health IT or a health information network/health information exchange, all as defined by the Information Blocking Rule at 45 C.F.R. § 171.102.

Applicable Law means federal and state statutes and regulations that apply to Organization.

Designated Record Set (DRS) means medical records, billing records, or any other group of records maintained by or for a covered health care provider to make decisions about individuals.

Electronic Access means an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request.

Electronic Health Information (EHI) means Electronic Protected Health Information contained in a Designated Record Set. It does not include Psychotherapy Notes or information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding. EHI also excludes any information that has been de-identified in accordance with HIPAA's de-identification standards. And until May 2, 2022, the definition of EHI may be further limited to those data elements represented in the USCDI (version 1).

Electronic Protected Health Information (ePHI) means individually identifiable health information (as defined by HIPAA) that is transmitted by electronic media or maintained in electronic media.

Exchange means the ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks.

Fee means any present or future obligation to pay money or provide any other thing of value.

HIPAA collectively refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations (see 45 C.F.R. Parts 160, 162, and 164), all as amended from time to time.

Information Blocking Rule collectively refers to 42 U.S.C. § 300jj-52 and its implementing regulations 45 C.F.R. Part 171.

Interoperability Element means hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that may be necessary to Access, Exchange or Use EHI; and are controlled by the Actor, which includes the ability to confer all rights and authorizations necessary to use the element to enable the Access, Exchange or Use of EHI.

Required by Law means a practice that is explicitly required by state or federal law, including statutes, regulations, court orders, binding administrative decisions or settlements, as well as tribal law (as applicable). Required by Law does **not** mean practices permitted by law or engaged in pursuant to a law, such as privacy laws that require an individual's consent or authorization prior to disclosing EHI to the requestor.

United States Core Data for Interoperability (USCDI) (version 1) means the standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange, which are published by The Office of the National Coordinator for Health Information Technology on its USCDI website.

Use means the ability for EHI, once Accessed or Exchanged, to be understood and acted upon.

SAFE HARBORS

If a practice falls within a Safe Harbor, it will not violate the Information Blocking Rule. **All of the regulatory conditions must be met in order for a Safe Harbor to apply.** More than one Safe Harbor may apply.

1. Preventing Harm Safe Harbor

So long as the conditions of the Preventing Harm Safe Harbor are met, it will not be information blocking if a practice substantially reduces a regulatory cognizable risk of harm to a natural person.

Application to individuals and legal representatives. Organization will follow its HIPAA Individual Access Policies and related procedures with respect to granting, delaying or denying an individual's (or legal representative's) request to access the individual's EHI, including any rights such individuals'/legal representatives' might have to have a denial determination reviewed and potentially reversed.

Application to other EHI requestors. For requestors other than an individual or legal representative, Organization may delay, deny, or otherwise interfere with the requestor's Access, Exchange or Use of EHI, if Organization holds a reasonable belief that the practice will substantially reduce a risk of harm to the life or physical safety of a natural person under one of the following circumstances:

- A licensed health care professional—who has a current or prior clinical-patient relationship with the individual whose EHI is affected—makes this risk of harm determination on an individualized basis and in the exercise of professional judgment; or
- This risk of harm arises from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason (collectively, "Corrupted Data"). An incomplete medical record or sporadic data entry errors do **not** constitute Corrupted Data.

Under either circumstance, Organization's practice will be no broader than necessary in order to substantially reduce the risk of harm to the life or physical safety of a natural person. This risk of harm must be reasonably likely to occur but for Organization's interference with the Access, Exchange or Use of EHI. The Workforce Member who makes the risk of harm determination will document this determination. If it is appropriate to do so, this documentation may be kept in the affected individual's medical record.

Organization will also follow other applicable Safe Harbors—such as the Content and Manner Safe Harbor or Infeasibility Safe Harbor—in circumstances where the Preventing Harm Safe Harbor applies to only a portion of the EHI requested but it is not feasible for Organization to provide Access, Exchange or Use of the rest of the requested EHI in the manner it is requested due to technical or administrative limitations (such as lacking data segmentation capabilities to sequester only the Corrupted Data).

Organization will implement its practices under this Safe Harbor (including any applicable HIPAA policies and procedures) in a consistent and non-discriminatory manner.

2. Privacy Safe Harbor

It will not be information blocking if Organization engages in privacy-related practices, so long as the conditions of the Privacy Safe Harbor are met.

Organization will follow its HIPAA Individual Access Policies and related procedures with respect to granting, delaying or denying an individual's (or personal representative's) request to access the individual's EHI, including those circumstances where the HIPAA right to access denial is not reviewable or it is not appropriate to treat a person as an individual's personal representative.

Organization will follow its HIPAA Use and Disclosure Policies and related procedures with respect to granting, delaying or denying a third-party's request for Access, Exchange or Use of EHI, including when a legal precondition must be met. Organization's practices are tailored to satisfy applicable legal preconditions and are implemented in a consistent and non-discriminatory manner. Examples of legal preconditions for compliance with health information privacy laws that apply to Organization include, but are not limited to:

- **Authorizations/consents.** Depending on who is requesting the EHI and for what purpose, Organization may be required by state or federal privacy laws to obtain a signed authorization or consent from the individual or the individual's personal representative. The state or federal privacy law might require that the authorization or consent used meet certain requirements. Organization has a policy or procedure that sets forth the necessary elements of any required authorizations or consents. When a requestor submits an authorization or consent that Organization determines pursuant to this policy or procedure is not valid, Organization will use reasonable efforts within its control to provide the requestor with a consent or authorization form that satisfies the requirements or otherwise provide reasonable assistance with respect to the deficiencies. Organization will not improperly encourage or induce an individual to withhold the authorization or consent.
- **Verification of identity and authority.** Organization may be required by state or federal privacy laws to verify the identity and authority of a person requesting access to EHI. Organization tailors its verification practices to meet legal requirements and health care industry standard security procedures (see the Security Safe Harbor).

Organization may also elect to not provide Access, Exchange or Use of EHI if the following conditions are met:

- The individual, who is the subject of the EHI, requests that Organization not provide such Access, Exchange or Use of the individual's EHI. Organization will not improperly encourage or induce an individual to make such a request. Organization will follow any applicable HIPAA policies and procedures when evaluating whether to grant the request.
- Organization will document the request within a reasonable time period after the request is made.
- Organization will implement any practice of granting an individual's request not to share EHI in a consistent and non-discriminatory manner.
- Organization may terminate an individual's request for a restriction only under one of the following circumstances:
    - The individual agrees to the termination in writing or requests the termination in writing;
    - The individual orally agrees to the termination and Organization documents the oral agreement; or
    - Organization informs the individual that it is terminating its agreement, except that such termination is not effective to the extent prohibited by Applicable Law and only applicable to EHI created or received after Organization has informed the individual of the termination.

Organization will also follow other applicable Safe Harbors—such as the Content and Manner Safe Harbor or Infeasibility Safe Harbor—in circumstances where the Privacy Safe Harbor applies to only a portion of the EHI requested, but it is not feasible for Organization to provide Access, Exchange or Use of the rest of the requested EHI due to technical or administrative limitations (such as lacking data segmentation capabilities to sequester only the EHI subject to the Privacy Safe Harbor).

3. Security Safe Harbor

It will not be information blocking if Organization engages in practices that protect the security of EHI, so long as the conditions of the Security Safe Harbor are met.

Organization will follow its HIPAA security policies, procedures and security risk analyses and risk management plans with respect to granting, delaying, denying or otherwise interfering with the provision of Access, Exchange or Use of EHI. Organization's security practices will be:

- Directly related to safeguarding the confidentiality, integrity, and availability of EHI;
- Tailored to the specific security risk being addressed; and
- Implemented in a consistent and non-discriminatory manner across similarly situated persons or entities whose interactions pose the same level of security risk.

In the event Organization's HIPAA security policies and procedures do not sufficiently address a known security risk, Organization will document its security practice based on particularized facts and circumstances surrounding the security risk, including:

- Why the security practice was necessary to mitigate the security risk to EHI; and
- That there were no reasonable and appropriate alternatives that would address the security risk and would be less likely to interfere with the Access, Exchange or Use of EHI. This last factor will be highly dependent on the urgency and nature of the security threat in question. In the event of exigent circumstances, Organization may implement in good faith a security practice without first considering whether there are reasonable and appropriate alternatives that are less likely to interfere with the Access, Exchange or Use of EHI. However, the initial-response practice may be in place for only a short time and contingent upon Organization more fully identifying and assessing current risks in context or as follow-up to the exigent circumstances. If appropriate, Organization will modify or replace its initial-response practice with a less onerous alternative that is reasonable and appropriately tailored to the specific risk addressed.

Organization also may (but is not required to) give individuals educational information about the privacy and security risks posed by third-party applications. Such educational information will not rise to the level of an interference with the Access, Exchange or Use of EHI so long as all three of the following requirements are met:

- The information focuses on current privacy and/or security risks of the technology or the third-party developer;
- The information is factually accurate, unbiased, objective, and is not unfair or deceptive; and
- The information is provided in a non-discriminatory manner.

Organization may provide this education through an automated attestation and warning process upon request from an individual to transmit data to a third-party application. **Organization will not prevent an individual from deciding to provide its EHI to a technology developer or third-party application despite any risks noted regarding the application itself or the third-party developer.**

Organization will not engage in security practices that have the practical effect of disadvantaging competitors or steering referrals.

4. Content and Manner Safe Harbor

Organization strives to fulfill requests for Access, Exchange or Use of EHI in the manner it is requested and in compliance with Applicable Law. If Organization fulfills such an EHI request in the manner it is requested any fees charged or licensing requirements imposed on the Interoperability Elements used are not required to comply with the Fees Safe Harbor or Licensing Safe Harbor. However, it will not be information blocking if Organization fulfills an EHI request in an alternative manner, so long as the conditions of the Content and Manner Safe Harbor are met.

Content Limitation. Until **May 2, 2022**, Organization may (but is not required to) limit its response to an EHI request to only those data elements represented by the data elements in the USCDI (v1) standard. This option will not be available after May 2, 2022.

Alternative Manner Option. Organization may respond to an EHI request in an alternative manner if one of the following circumstances applies:

- Organization is technically unable to fulfill the request; or
- Organization is unable to reach agreeable terms with the requestor.

If Organization is technically unable to fulfill the request in the manner requested or cannot reach agreeable terms with the requestor, Organization will fulfill the request in an alternative manner and without unnecessary delay, unless it is infeasible for Organization to do so (see the Infeasibility Safe Harbor). Organization will notify the requestor within **10 business days of the request** if fulfilling the EHI request in the manner requested or in an alternative is infeasible.

If responding in an alternative manner is feasible, Organization will technically fulfill the request using the technical standards listed below in the following order of priority, only proceeding to the next technical standard if Organization is technically unable to fulfill the request using the higher priority standard:

- Using certified technology specified by the requestor (*e.g.*, via application programming interface (API), Direct protocol);
- Using content and transport standards specified by requestor and published by the federal government or standards development organization accredited by the American National Standards Institute (ANSI); or
- Using an alternative machine-readable format agreed upon with the requestor (*e.g.*, Portable Document Format (PDF), comma-separated value (CSV) files).

Organization may also require the requestor to first agree to licensing terms for the Interoperability Elements and/or fees in accordance with the Licensing Safe Harbors and Fees Safe Harbor. If applicable, Organization will begin negotiating any licensing terms within **10 business days of the request** and offer a **negotiated license within 30 business days of the request**.

5. Infeasibility Safe Harbor

It will not be information blocking if Organization faces legitimate practical challenges that may limit Organization's ability to comply with a request for Access, Exchange or Use of EHI, so long as the conditions of the Infeasibility Safe Harbor are met. If Organization makes an infeasibility determination for any of the three reasons stated below, Organization will notify the requestor of the infeasibility determination in writing—including the reason(s) for the infeasibility determination—**within 10 business days of the EHI request**.

It may be infeasible for Organization to fulfill a request for Access, Exchange or Use of EHI under the following circumstances:

- **Uncontrollable Events.** Organization may not be able to fulfill an EHI request 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.
- **Data Segmentation.** Organization may not be able to fulfill an EHI request because Organization cannot unambiguously segment the requested EHI from EHI that cannot be disclosed due to an individual's privacy preferences or legal requirements (see the Privacy Safe Harbor), or because the EHI may be withheld under the Preventing Harm Safe Harbor.
- **Infeasible under the Circumstances.** Organization may determine based on the following factors that complying with the EHI request is not feasible:
    - The type of EHI and the purposes for which it may be needed;
    - The cost of complying with the request in the manner requested;
    - The financial and technical resources available to Organization;
    - Whether Organization's practice is nondiscriminatory in its application to others with whom Organization has a business relationship;
    - Whether Organization owns or has control over a predominant technology or platform through which the EHI is Accessed or Exchanged; and
    - Why Organization could not make the EHI available under the Content and Manner Safe Harbor.

  In making such a determination, Organization must **not** consider any of the following factors:
    - Whether complying with the EHI request in the manner requested would facilitate competition with Organization;
    - Whether complying with the EHI request would prevent Organization from charging a fee or will result in a reduced fee to Organization.

  Organization will document its consideration of these factors in writing and prior to responding to the EHI request. Organization will apply these factors consistently and in a non-discriminatory manner.

6. Fees Safe Harbor

Organization is not required to comply with the Fees Safe Harbor if Organization is able to provide Access, Exchange or Use of EHI in the manner it is requested under the conditions of the Content and Manner Safe Harbor. However, if Organization will respond to the EHI request in an alternative manner, Organization will not violate the Information Blocking Rule by charging a reasonable fee, so long as conditions of the Fees Safe Harbor are met. **This Safe Harbor does not permit or support the sale of EHI.**

Organization will follow its HIPAA Individual Access Policies and related procedures with respect to any fees charged to an individual's (or personal representative's) request to access the individual's EHI. **Organization will not charge any fees that are prohibited by HIPAA or 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.** For example, Organization will not charge fees for Electronic Access if an individual directs Organization to disclose the individual's EHI to a biomedical research program, a personal health application or a personal health record of the individual's choosing.

For requestors other than an individual or personal representative, Organization may (but is not required to) impose a fee on the Access, Exchange or Use of EHI, so long as the fee is based on the following:

- Objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;

- Reasonably related to Organization'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;
- 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
- Costs not otherwise recovered for the same instance of service to a provider and third-party.

Any fees charged will **not** be based on any of the following *(if applicable)*:

- Whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with Organization;
- 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;
- Costs Organization 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 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;
- Any costs that led to the creation of intellectual property, if Organization charged a royalty for that intellectual property under the Licensing Safe Harbor and that royalty included the development costs for the creation of the intellectual property; or
- Fees to perform an export of EHI via certified health IT for the purposes of switching health IT or to provide patients their EHI, or 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.

7. Licensing Safe Harbor

Organization is not required to comply with the Licensing Safe Harbor if Organization is able to provide Access, Exchange or Use of EHI in the manner it is requested under the conditions of the Content and Manner Safe Harbor. However, if Organization will respond to the EHI request in an alternative manner, Organization will not violate the Information Blocking Rule by imposing terms and conditions (*e.g.*, a license or non-disclosure agreement) on the requestor's use of Interoperability Elements to Access, Exchange or Use EHI, if the requirements of the Licensing Safe Harbor are met.

In the event Organization licenses the use of Interoperability Elements to Access, Exchange or Use EHI in an alternative manner, Organization will:

- Begin license negotiations with a requestor within **10 business days of the request**; and
- Negotiate in good faith a license within **30 business days of the request**.

The license will meet all of the following requirements (*as applicable*):

- **Scope of License.** It will provide all rights necessary to enable the Access, Exchange or Use of EHI achieve the intended Access, Exchange or Use of EHI via the Interoperability Elements.
- **Royalty.** If a royalty is charged, the royalty will be reasonable, non-discriminatory and based solely on the independent value of Organization's technology to the licensee's products. A royalty will not be based on any strategic value stemming from Organization's control over essential means of Accessing, Exchanging, or Using EHI. If Organization has licensed the Interoperability Element through a standards developing organization, Organization may charge a royalty that is consistent with such policies. However, Organization will not charge a royalty for intellectual property if Organization recovered any development costs that led to the creation of the intellectual property.

- **Non-Discriminatory**. The licensing terms will be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons and requests. **The terms will not be based on whether the requestor or other person is a competitor, potential competitor, or will be using EHI obtained in a way that facilitates competition with Organization or the revenue or other value the requestor may derive from the Access, Exchange or Use of EHI obtained via the Interoperability Elements**.
- **Collateral Terms.** Organization will not require the requestor to do any of the following:
    - Execute a non-compete in any product, service, or market;
    - Deal exclusively with Organization in any product, service, or market;
    - Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested Interoperability Elements;
    - License, grant, assign, or transfer to Organization any intellectual property of the licensee; or
    - Pay a fee of any kind unless the Fees Safe Harbor is met.

If Organization will require the use of a non-disclosure agreement in connection with the use of Interoperability Elements to Access, Exchange or Use EHI, the NDA must meet the following requirements:

- It must be reasonable; and
- No broader than necessary to prevent the unauthorized disclosure of Organization's trade secrets. The information Organization claims as trade secrets must be stated with particularity in the NDA and such information must meet the definition of a trade secret under Applicable Law.

Finally, when provisioning a requestor with use of Organization's Interoperability Elements, Organization will not engage in any practice that has any of the following purposes or effects:

- Impedes the efficient use of the Interoperability Elements to Access, Exchange or Use EHI for permissible purposes;
- Impedes the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand; and/or
- Degrade the performance or interoperability of the licensee's products or services, unless necessary to improve Organization's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

EDUCATION AND TRAINING ON THE INFORMATION BLOCKING RULE

Organization will provide appropriate training to Workforce Members on this policy and the Information Blocking Rule. Organization will perform this training on a periodic and ongoing basis.

1. Initial Training

Organization will ensure Workforce Members receive training appropriate to the Workforce Member's position and responsibilities concerning the Information Blocking Rule. All Workforce Members will participate in training when requested by Organization.

2. Periodic and Ongoing Training

Workforce Members will receive periodic or updated training concerning the Information Blocking Rule appropriate to the Workforce Member's position and responsibilities. If there is a material change in this policy, Organization will provide re-training to all affected Workforce Members within a reasonable period of time after the effective date of the material change. Organization's Privacy Official will determine the frequency of training, which may differ for certain Workforce Members depending on the Workforce Member's role and responsibilities. Compliance and education are an ongoing process and any compliance issues will be addressed as they arise.

3. Training and Education Format and Content

Organization will prepare education and training materials tailored to Workforce Members' organizational role, level of education, primary language, and that are mindful of cultural diversity.

Workforce Members will receive a copy of this No Information Blocking Policy and Organization's HIPAA policies and procedures.

Workforce Members will be educated on the Information Blocking Rule and the Safe Harbors applicable to Organization. Organization will instruct Workforce Members on how to identify and report non-compliance with this No Information Blocking Policy and the Information Blocking Rule. Workforce Members will be informed of Organization's sanctions policy for non-compliance with this No Information Blocking Policy, the Information Blocking Rule and Organization's HIPAA policies. Training also will address any changes in relevant laws or organizational policy and procedures.

Workforce Members will be provided an opportunity to ask questions and receive answers. Organization will encourage Workforce Members to ask questions as they arise after the conclusion of training.

Upon completion of training, Workforce Members will complete an assessment evaluating their comprehension of this No Information Blocking Policy and the Information Blocking Rule. Organization also will maintain a written record of the content of any training provided and a written acknowledgement by the Workforce Members that they participated in the training. The written acknowledgement may be in the form of the Workforce Member's signature on a sign-in sheet or any other written form that the Workforce Member signs.

INFORMATION BLOCKING REPORTING

1. Information Blocking Reporting and No Retaliation

Workforce Members that reasonably believe Organization or one of its Workforce Members (including any affiliate, agent or vendor) is violating this No Information Blocking Policy or the Information Blocking Rule must promptly notify Organization. Anonymous reports may be made by depositing the report in the designated compliance report lock box.

Organization will not retaliate against any Workforce Member for reporting a suspected or actual violation of this No Information Blocking Policy or the Information Blocking Rule.

2. Investigations

Organization's Privacy Official (or designee) will respond to all allegations of information blocking and, where appropriate, investigate such allegations within a reasonable period of time.

As part of the investigation, the Privacy Official (or designee) will:

- Identify all persons who were involved in the alleged information blocking practice and interview them;
- Identify, review and preserve all relevant documentation, including relevant policies and procedures, e-mails, correspondence, notes, files and other documents that may have been created by those involved in the matter;
- Assess whether the practice complained of implicates the Information Blocking Rule and whether the practice is Required by Law or falls into one or more Safe Harbors;
- Address and mitigate any compliance issues, including but not limited to disciplining any Workforce Members who have violated this No Information Blocking Policy or the Information Blocking Rule; and
- Document all of the above, including the final disposition of the complaint and any disciplinary actions.

3. Compliance Evaluations

Organization will solicit information from Workforce Members and encourage questions and feedback concerning this No Information Blocking Policy and the Information Blocking Rule. Organization will amend policies, procedures, practices and training where necessary, on an ongoing basis, to comply with the Information Blocking Rule.

4. Sanctions

Organization may discipline Workforce Members who violate this No Information Blocking Policy or the Information Blocking Rule, including Workforce Members who:

- Fail to report actual or suspected violations of this No Information Blocking Policy or the Information Blocking Rule; or
- Who engage in retaliatory behavior.

Organization will discipline Workforce Members in accordance with its sanctions policies and procedures. The level of disciplinary action imposed will depend on the severity of the violation and may include termination of employment or association with Organization.

RELATED DOCUMENTS

Organization's HIPAA Individual Access Policies and related procedures
Organization's HIPAA Use and Disclosure Policies and related procedures

APPROVAL HISTORY

This policy will remain in effect unless terminated or superseded by a revised and/or updated policy issued by Organization. This policy was reviewed and, if applicable, revised by Workforce Members with the relevant clinical, technical, legal or other appropriate expertise.

APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR

LEGAL REFERENCES

42 U.S.C. § 300jj-52
45 C.F.R. Part 171
ONC Cures Act Final Rule (85 Fed. Reg. 25462)
United States Core Data for Interoperability, Version 1 (Feb. 2020)