[Name of Practice]

NO INFORMATION BLOCKING POLICY

Effective Date: April 5, 2021

Background Information

On December 13, 2016, the *21st Century Cures Act* (Cures Act) was signed into law. On May 1, 2020, the Office of National Coordinate issued the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (Information Blocking Rule)*[i], which implements provisions of the Cures Act that are designed to advance interoperability; support the seamless exchange, access, and use of electronic health information (EHI); and to address information blocking. The Cures Act also gives the HHS Office of Inspector General (OIG) authority to investigate claims of information blocking and assess civil monetary penalties against certain actors that engage in information blocking. The information blocking compliance effective date originally set for November 2, 2020 was extended to April 5, 2021.

Purpose

The purpose of this Policy is to outline PRACTICE's commitment to facilitating the timely access, exchange and use of electronic health information (EHI)[ii] in compliance with applicable law. This policy is related to PRACTICE's HIPAA Privacy and Security Policies and supports provision of informed care for patients by removing obstacles they encounter when trying to access, exchange, or use their own EHI.

The information blocking prohibition and other requirements discussed in this Policy derive from a legal regime similar to, but distinct from, HIPAA. Therefore, PRACTICE is implementing a separate policy and compliance initiatives related to information blocking.

Statement of Policy

PRACTICE is committed to making EHI available and usable for authorized and permitted purposes in accordance with applicable law. This Policy focuses on information blocking and the eight (8) exceptions that identify reasonable and necessary practices and activities that do not constitute information blocking.

Workforce Members are prohibited from engaging in practices 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, "Exceptions"). **The Information Blocking Rule does not require PRACTICE to disclose EHI if doing so would violate other Applicable Law, such as HIPAA or other state or federal laws.**

Application of this Policy

This Policy applies to all PRACTICE Personnel and Workforce Members as those terms are defined in PRACTICE's HIPAA Privacy and Security Policies. PRACTICE's Privacy Official has general responsibility for implementation of this Policy. The Information Blocking Rule is intent based. This means failure to satisfy an Exception does not mean that there is a violation of the Rule. However, PRACTICE strives to satisfy the conditions of any applicable Exception when engaging in practices that might implicate the Information Blocking Rule. Therefore, 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 PRACTICE has control.

Data that Must be Provided

Patients must have access to their EHI by April 5, 2021. For the first 18 months after the rule goes into effect, EHI refers to the information contained in the data classes set forth in the United States Core Data for Interoperability (USCDI) standard.

USCDI contains a set of 16 data classes:

- Patient Demographics
- Vital Signs
- Allergies and Intolerances
- Medications
- Smoking Status
- Immunizations
- Procedures
- Care Team Members
- Clinical Notes
- Assessment and Plan of Treatment
- Goals
- Health Concerns
- Laboratory
- Problems
- Unique Device Identifiers (for a patient's Implantable Device)
- Provenance (i.e. the metadata of the records provided)

Each data class includes specific data elements that must be provided upon patient request. For example, the data class for Clinical Notes includes 8 different types of notes that must be made available to patients: consultation notes; discharge summary notes; history & physical notes; imaging narratives; laboratory report narratives; pathology report narratives; procedure notes; and progress notes.

After October 6, 2022, the scope of EHI under the information blocking rule will expand to include the full electronic designated record set (DRS) as defined in HIPAA. Healthcare providers will be obligated to provide not only the USCDI information listed above, but also DRS data which includes:

- medical & billing records about individuals maintained by or for a covered health care provider;
- enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

This last category includes records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access.

Information Blocking Exceptions

The Information Blocking Rule outlines eight (8) detailed practices and activities that will not constitute information blocking even if they do in fact interfere with the access, exchange, or use of EHI. The eight Exceptions to information blocking fall into two categories, each of which has detailed requirements: 1) Exceptions that involve *not fulfilling requests* to access, exchange, or use EHI and 2) Exceptions that involve *procedures for fulfilling requests* to access, exchange, or use EHI.

All of the regulatory conditions must be met in order for an Exception to apply.

Five Exceptions – Not Filling Requests

1. **Preventing harm exception**: For a requester other than the individual patient or his/her legal representative, PRACTICE may delay, deny or otherwise interfere with the requestor's access, exchange or use of EHI if PRACTICE holds a reasonable belief that doing so will substantially reduce a risk of harm to the life or physical safety of a natural person under one of the following circumstances:
   a. A licensed health care professional -who has a current or prior clinical 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
   b. 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").[iii]

2. **Privacy exception**: PRACTICE may delay or deny an individual's or personal representative's request to access the individual's EHI if doing so is permitted by and consistent with PRACTICE's HIPAA Privacy and Security Policies related to individual access and use and disclosures.[iv]

3. **Security exception**: PRACTICE may delay, deny or otherwise interfere with a requester's access to EHI if doing so protects the security of EHI and is consistent

with PRACTICE's security policies, procedures, and security risk analysis and management plans.[v] PRACTICE will not prevent an individual from deciding to provide his/her EHI to a technology developer or third-party application despite any risk noted regarding the application itself or the third-party developer.

4. **Infeasibility exception**: PRACTICE does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request. If PRACTICE makes an infeasibility determination for any of the three reasons listed below, PRACTICE 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.**[vi] It may be infeasible for PRACTICE to fulfill a request for access, exchange or use of EHI under the following circumstances:
    a. **Uncontrollable Events:** PRACTICE 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.
    b. **Data Segmentation:** PRACTICE may not be able to fulfill an EHI request because PRACTICE cannot unambiguously segment the requested EHI from EHI that cannot be disclosed due to an individual's privacy preferences or legal requirements.
    c. Infeasible under the Circumstances: PRACTICE may determine, based on the following factors, that complying with the EHI request is not feasible:
        i. The type of EHI and the purposes for which it may be needed
        ii. The cost of complying with the request in the manner requested;
        iii. The financial and technical resources available to the organization;
        iv. Whether PRACTICE's practice is nondiscriminatory in its application to others with whom PRACTICE has a business relationship
        v. Whether PRACTICE owns or has control over a predominant technology or platform through which the EHI is accessed or exchanged; and
        vi. Why PRACTICE could not make the EHI available under the "Content and Manner" exception.

5. **Health IT performance exception**: PRACTICE will not be engaged in information blocking if it temporarily makes unavailable health IT for updates and other improvements o long as such unavailability is intended to maintain and improve the health IT, consistent with existing service level agreements, intended to

prevent harm under the Preventing Harm exception, or security-related under the Security Exception.[vii]

Three Exceptions – Fulfilling Requests

1. **Content and manner exception**: PRACTICE may fulfill an EHI request in an alternative manner, if one of the following circumstances applies:

   a. PRACTICE is technically unable to fulfill the request; or
   b. PRACTICE is unable to reach agreeable terms with the requestor. PRACTICE will notify the requestor within **10 business days of the request** and offer if fulfilling the EHI request in the manner requested or in an alternative manner is infeasible[viii].

2. **Fees exception**: If PRACTICE will respond to the EHI request in an alternative manner (as permitted by the Content and Manner Exception), PRACTICE will not violate the Information Blocking Rule by charging a reasonable fee. **This exception does not permit or support the sale of EHI. PRACTICE will not charge any fees that are prohibited by HIPAA or based in any part on the electronic access of an individuals' EHI by the individual, their personal representative, or another person or entity designated by the individual.[ix]**

3. **Licensing exception**: If PRACTICE will respond to the EHI request in an alternative manner (as permitted by the Content and Manner Exception), PRACTICE 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. In the event PRACTICE license the use of interoperability elements to access, exchange or use EHI in an alternative manner, PRACTICE will (a) 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. "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 GSPCH which includes the ability to confer all rights and authorizations necessary to sue the element to enable the access, exchange or use of EHI. [x]

Operational Requirements

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

2. **Reporting and No Retaliation.** Workforce Members that reasonably believe PRACTICE or one of its Workforce Members is violating this Policy or the Information Blocking Rule must promptly notify PRACTICE. PRACTICE will not retaliate against any Workforce Member for reporting a suspected or actual violation of this Policy or the Information Blocking Rule.

3. **Investigations**. The PRACTICE Privacy Official (or designee) will respond to all allegations of information blocking and, where appropriate, investigate such allegations within a reasonable period of time.

4. **Sanctions**. PRACTICE may discipline Workforce Members who violate this Policy or the Information Blocking Rule, including Workforce Members who (a) fail to report actual or suspected violations of this Policy or the information Blocking Rule; or (b) who engage in retaliatory behavior. The level of disciplinary action imposed will depend on the severity of the violation and may include termination of employment or association with PRACTICE.

5. **Documentation.** If this Policy requires an action, activity, or assessment to be documented, PRACTICE will maintain a written record of the action, activity or assessment and will retain such documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

---

[i] Information Blocking Final Rule, 85 Fed Reg. 25642. The Safe Harbors are specifically discussed at Section VIII(D), pages 25820-25900

[ii] In the Information Blocking Rule, the ONC aligned the definition of EHI with HIPAA's electronic protected health information (EPHI) that would be included in a designated record set. Thus, electronic health information (EHI) means EPHI as defined in 45 CFR § 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR § 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR § 160.103.

[iii] 45 CFR § 171.201

[iv] 45 CFR § 171.202

[v] 45 CFR § 171.203

[vi] 45 CFR § 171.204

[vii] 45 CFR § 171.205

[viii] 45 CFR §171.301

[ix] 45 CFR §171.302

[x] 45 CFR §171.303