Envision HEALTHCARE	Ethics & Compliance Department		
	Policy No.: 77	**Created:**	02/2021
		Reviewed:	09/2024
		Revised:	

HIPAA: INFORMATION BLOCKING

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare Operating, Inc. and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Information Blocking policy to (i) address the effect of the Information Blocking Rules on disclosures of EHI (as defined below) permitted by HIPAA and these HIPAA policies; (ii) describe a process for determining whether such disclosures are required by the Information Blocking Rules; and (iii) describe a process for determining whether any exceptions to the Information Blocking Rules permit the Company to deny a request for EHI otherwise permitted by HIPAA.

DEFINITIONS:

A. *Electronic Health Information ("EHI")* means electronic protected health information included in a designated record set (as defined by HIPAA), regardless of whether the group of records are used or maintained for a Covered Entity. EHI does not include: (i) psychotherapy notes (as defined in 45 CFR 164.501); or (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. EHI excludes de-identified information.

B. *Information Blocking Rules* means the rules prohibiting practices likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI held on behalf of a covered entity or any other entity as set forth at 45 CFR § 171.100, *et seq*.

C. *Practice* means an act or omission by the Company. For purposes of this policy, examples of Practices include denying requests to access, use, or exchange EHI; charging fees for access, exchange, or use of EHI; or the manner in which access, use, or exchange of EHI is provided.

POLICY:

The Company is committed to exchanging and making EHI available and usable for authorized and permitted purposes in accordance with applicable law. Accordingly, the Company shall seek to not engage in Practices that are likely to interfere with the access, exchange or use of EHI except

as required by law, permitted by an information blocking exception, or otherwise permitted by the Information Blocking Rules.

The Company's Practices, including uses and disclosures of EHI, must be in accordance with the HIPAA Policies, HIPAA, and the Information Blocking Rules. Whereas HIPAA *permits* the Company to access, use, and exchange EHI for certain purposes, the Information Blocking Rules *require* the Company to do so unless an exception applies or the Actor can otherwise demonstrate that the Practice complies with the Information Blocking Rules (such as a Practice by a health care provider that is reasonable or a Practice that the health care provider did not know would interfere with the access, exchange, or use of EHI).

A Practice that does not meet all of the requirements of an exception does not automatically constitute a violation of the Information Blocking Rules. To be considered information blocking, the Company must know that such Practice is unreasonable and is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI.

When the Company receives a request for EHI (for example: a patient requests access to or a copy of their EHI; an unaffiliated treating provider requests information relating to a patient's health outcomes; a health plan requests information relating to a member's claims) or otherwise engages in a Practice (for example: having a policy in place that patient consent is required to share EHI with other treating providers, even if permitted by law without consent; requiring community physicians to adopt the same EMR as Company or otherwise revoking admitting privileges), if the Practice is able to meet an exception, as defined below, it will not be considered information blocking as the exceptions act as "safe harbors" under the Information Blocking Rules.

Exceptions: If the Company receives a request for EHI, and the requested access, exchange, use, or disclosure is permitted by HIPAA but not required by HIPAA or other law, the Company may deny the request or otherwise engage in a Practice with respect to such EHI if one of the exceptions set forth below is met:

A. Preventing Harm Exception (for Practices that substantially reduce a risk of harm to a patient or another natural person);

B. Privacy Exception (for Practices intended to protect an individual's privacy, such as obtaining an authorization that complies with HIPAA or applicable state law or honoring a patient's wishes not to share Protected Health Information);

C. Security Exception (for Practices to protect the security of EHI);

D. Infeasibility Exception (for Practices that are due to a request for EHI being infeasible, such as due to a disaster, an inability to segment data or factors such as cost);

a. If the Company denies a request for EHI based on the Infeasibility Exception, the Company shall, within ten (10) business days of the request, provide to the requestor in writing an explanation of why the request is infeasible (e.g., uncontrollable events, segmentation restrictions, or circumstances otherwise making the request infeasible).

E. Health IT Performance Exception (for Practices implemented to perform maintenance or improvements to health IT or to address a third-party application that is negatively impacting the health IT's performance);

F. Content and Manner Exception (for Practices tied to providing EHI in the manner requested or through an alternative);

G. Fees Exception (for Practices involving charging fees in connection with exchanging EHI); and

H. Licensing Exception (for Practices involving licensing interoperability elements needed to exchange EHI).

Requests to access, exchange, or use EHI must be evaluated promptly. Third parties requesting to access, exchange, or use EHI may be asked to clarify the content, manner, and/or purpose of the request to assist the Company with confirming:

A. That the potential access, exchange, or use is permitted by law;

B. Whether the Company can furnish the requested EHI content; and

C. Whether the Company can provide the EHI in the manner requested. Alternatives to the content and/or manner requested will be identified and offered when necessary, in accordance with Company guidance.

Teammates who have questions about whether any exceptions to the Information Blocking Rules apply should contact the Privacy Official before denying requests for access, exchange, or use of EHI or otherwise implementing a Practice.

The Privacy Official will document details regarding any decision-making process when denying requests to access, exchange, or use EHI (or otherwise engaging in a Practice) when an exception does not apply. Practices that may impact the sharing of EHI are permitted if they are necessary to comply with other Company policies, such as the Company's HIPAA Policies regarding uses and disclosures of PHI that are permitted under HIPAA, but Company guidance should be consulted to confirm the request is responded to in a manner that demonstrates compliance with an exception or otherwise complies with the Information Blocking Rules.

Information that is required to be documented by this policy or is otherwise created to demonstrate compliance with an exception shall be recorded and be maintained for six (6) years from the date of its creation or the date it is last in effect, as applicable.

The process outlined in this policy must be followed in a manner consistent with the Company's other HIPAA policies regarding the use and disclosure of PHI. For example, the minimum necessary standard applies, as described in *HIPAA Policy #4 – HIPAA: Minimum Necessary / Need to Know*; (ii) the identification rules outlined in *HIPAA Policy #38 – HIPAA: Verification of Person(s) Requesting Protected Health Information* apply, and (iii) the safeguards outlined in *HIPAA Policy #51 – HIPAA: Safeguards* must be observed.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.