Title/Subject: HIPAA: INFORMATION BLOCKING

Applies to: ☒Faculty ☒Staff ☐Students ☐Student Employees ☐Visitors ☒Contractors

Effective Date of This Revision: June 27, 2025

Contact for More Information: Office of HIPAA Compliance
989-774-2829
HIPAA@cmich.edu

☐Board Policy ☒Administrative Policy ☐Procedure ☐Guideline

BACKGROUND:

The 21st Century Cures Act, Pub. L. 114-255, as it may be amended, advances interoperability and addresses information blocking. Sharing electronic health information (EHI) is the norm in healthcare, and only reasonable and necessary activities defined by the Secretary of Health and Human Services (HHS) may be used to block information sharing.

PURPOSE:

Central Michigan University (CMU) and its Hybrid Entity is committed to making EHI available and usable for authorized and permitted purposes in accordance with applicable law. This Policy focuses on removing obstacles patients encounter when trying to access their own EHI. This Policy will also deter information blocking faced by healthcare providers when providing informed care to patients. Specifically, 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.

DEFINITIONS:

Actor: A health care provider, health IT developer of certified health IT, health information network or health information exchange.

Information Blocking: Any practice by an Actor that is likely to interfere with the access, exchange, or use of electronic health information (EHI), except as required by law or specified in an information blocking exception.

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 electronic health information; and is/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 electronic health information.

Workforce Member: includes employees, volunteers, students, trainees, and other persons whose conduct, in the performance of work for a unit in the CMU Hybrid Entity is under the direct control of such entity, whether or not they are paid by the entity. This includes students at a CMU work-site who have access to PHI in order to satisfy a clinical experience requirement for a program of study.

All other terms used in this policy have the same meaning as those terms in the regulations at 45 CFR Part 171.

POLICY:

I. CMU prohibits Information Blocking practices that do not meet all conditions justifying an exception as outlined in this Policy.

II. CMU shall make all EHI available to patients in a reasonable and permissible timeframe unless an allowable exception applies. CMU shall further make EHI available upon request in electronic or other forms and formats unless an allowable exception applies.

III. The Cures Act outlines eight (8) exceptions whereby Information Blocking is permissible. Practices or activities that satisfy one of more of these exceptions, will not be considered Information Blocking if all the criteria of the applicable exception(s) are strictly met.

IV. Preventing harm exception: CMU may engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided the below conditions are met:

a. CMU holds a reasonable belief that the practice will substantially reduce a risk of harm;

b. The practice is no broader than necessary;

c. The practice satisfies at least one condition from each of the following four elements:

1. Type of risk

i. The risk of harm has been determined on an individualized basis in the exercise of professional judgements by a licensed health care provider who has a current or prior clinical relationship with the patients whose EHI is affected by the determination; or

ii. The risk of harm has arisen from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

2. Type of harm

i. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person, and the practice is likely to, or in fact does, interfere with the patient's access, exchange, or use of the patient's own EHI; or the practice is likely to, or in fact does, interfere with a legally permissible access, exchange, or use of EHI, regardless of whether the risk of harm the practice is intended to reduce is consistent with Section IV(c)(1) of this section; or

ii. The PHI makes reference to another person (unless such other person is a Health Care Provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person, and the practice is likely to, or in fact does, interfere with the patient's or their legal representative's access to, use or exchange of information that references another person and the practice is implemented pursuant to an individualized determination of risk of harm consistent with Section IV(c)(1)(i) of this section; or

iii. The request for access is made by the individual's legal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such legal representative is reasonably likely to cause substantial harm to the individual or another person, and the practice is likely to, or in fact does, interfere with access, exchange, or use of the patient's EHI by the legal representative and the practice is implement pursuant to an individualized determination of risk of harm consistent with Section IV(c)(1)(i) of this section.

3. Patient right to request review of individualized determination of risk of harm. Where the risk of harm is consistent with Section IV(c)(1)(i) of this section, CMU must implement the practice in a manner consistent with any rights the individual patient whose electronic health information is affected may have under 45 CFR § 164.524(a)(4), or any applicable Federal, State, or tribal law, to have the determination reviewed and potentially reversed.

4. Practice implemented based on an organizational policy or a determination specific to the facts and circumstances. The practice must be consistent with an organizational policy that meets Section IV(c)(4)(i) below or, in the absence of an organizational policy applicable to the practice or to its use in particular circumstances, the practice must be based on a specific determination that meets Section IV(c)(4)(ii) below.

i. Organizational Policy: A CMU written policy that is based on relevant clinical, technical, and other appropriate expertise, is implemented in a consistent and non-discriminatory manner, and meets all other applicable conditions; or
ii. Specific Determination: A determination based on facts and circumstances known or reasonably believed by CMU at the time of the determination and while the practice remains in use and based on expertise relevant to implementing the practice in a way that meets all other applicable conditions.

V. Privacy exception: CMU may engage in Information Blocking or otherwise not fulfill requests to access, exchange, or use EHI in order to protect an individual's privacy, provided the following conditions are met:
   a. Precondition not satisfied: State or Federal law, including the HIPAA Privacy Rule, require one or more preconditions for providing access, exchange, or use of PHI that have not been satisfied, and all of the following:
      1. CMU's practice is tailored to the applicable precondition not satisfied, is implemented in a consistent and non-discriminatory manner, and either conforms to written CMU's policies and procedures that specify the criteria to be used to determine when the precondition would be satisfied, and the steps CMU will take to satisfy the precondition; and
      2. Are documented, on a case-by-case basis, identifying the criteria used to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and
      3. If the precondition relies on the provision of a consent or authorization from an individual and CMU has received a version of such a consent or authorization that does not satisfy all elements of the precondition required under applicable law, then CMU must:
         i. Use reasonable efforts within its control to provide the individual with a consent or authorization form that satisfies all required elements of the precondition or provide other reasonable assistance to the individual to satisfy all required elements of the precondition; and
         ii. Not improperly encourage or induce the individual to withhold the consent or authorization.
   b. Denial of an individual's request for their EHI is consistent with the HIPAA Privacy Rule.
   c. Respecting an individual's request not to share information: CMU may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided the following conditions are met:
      1. The individual requests that CMU not provide such access, exchange, or use of electronic health information without any improper encouragement or inducement of the request by CMU;
      2. CMU documents the request within a reasonable time period;
      3. CMU's practice is implemented in a consistent and non-discriminatory manner; and
      4. CMU may terminate an individual's request for a restriction to not provide such access, exchange, or use of the individual's electronic health information only if:
         i. The individual agrees to the termination in writing or requests the termination in writing;
         ii. The individual orally agrees to the termination and the oral agreement is documented by CMU; or
         iii. CMU informs the individual that it is terminating its agreement to not provide such access, exchange, or use of the individual's electronic health information except that such termination is:
            a. Not effective to the extent prohibited by applicable Federal or State law; and
            b. Only applicable to electronic health information created or received after CMU has so informed the individual of the termination.

VI. Security exception: CMU may interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided the below conditions are met:
   a. The practice must be:
      1. Directly related to safeguarding the confidentiality, integrity, and availability of EHI; and

2. Tailored to specific security risks; and
3. Implemented in a consistent and non-discriminatory manner.

b. The practice must either:
   1. Implement a written CMU security policy that has been prepared on the basis of, and is directly responsive to, security risks identified and assessed by or on behalf of CMU, aligns with one or more applicable consensus-based standards or best practice guidelines, and provides objective timeframes and other parameters for identifying, responding to, and addressing security incidents; or
   2. where a written CMU security policy does not apply, be based on a determination in each case, based on the particularized facts and circumstances, that the practice is necessary to mitigate the security risk to EHI and there are no reasonable and 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.

VII. Infeasibility exception: CMU is not engaging in a practice of Information Blocking when it does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, provided the below conditions are met:

a. The practice must meet one of the following conditions:
   1. Uncontrollable events: CMU cannot fulfill the request for access, exchange, or use of EHI due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
   2. Segmentation: CMU cannot fulfill the request for access, exchange, or use of EHI because CMU cannot unambiguously segment the requested EHI.
   3. Infeasibility under the circumstances: CMU demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.

b. CMU provides a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

VIII. Health IT performance exception: CMU may take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided the below conditions are met:

a. The practice must:
   1. Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
   2. Be implemented in a consistent and non-discriminatory manner; and
   3. Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN.

b. CMU may take action against a third-party app that is negatively impacting the health IT's performance, provided that the practice is:
   1. For a period of time no longer than necessary to resolve any negative impacts;
   2. Implemented in a consistent and non-discriminatory manner; and
   3. Consistent with existing service level agreements, where applicable.

c. If the unavailability is in response to a risk of harm or security risk, CMU must only comply with the Preventing Harm or Security Exception, as applicable.

IX. Content and manner exception: CMU may limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided the below conditions are met:

a. Content Condition: Establishes the content CMU must provide in response to a request to access, exchange, or use EHI in order to satisfy the exception. CMU must respond to all requests to access, exchange, or use EHI.
    1. Up to 24 months after the publication date of the Cures Act final rule, an Actor must respond to a request to access, exchange, or use EHI with, at a minimum, the EHI identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard.
    2. On and after 24 months after the publication date of the Cures Act final rule, an Actor must respond to a request to access, exchange, or use EHI with EHI as defined in 45 CFR § 171.102, as it may be amended.

b. Manner Condition: Establishes the manner in which CMU must fulfill a request to access, exchange, or use EHI in order to satisfy this exception.
    1. CMU may need to fulfill a request in an alternative manner when CMU is:
        i. Technically unable to fulfill the request in any manner requested; or
        ii. Cannot reach agreeable terms with the requestor to fulfill the request.
    2. If CMU fulfills a request in an alternative manner, such fulfillment must comply with the order of priority described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

X. Fees exception: Notwithstanding the foregoing, CMU may charge fees, including fees that result in a reasonable profit margin in compliance with Michigan law, for accessing, exchanging, or using EHI, provided the below conditions are met:

a. Basis for fees condition. The fees CMU charges must be:
    1. Based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and request;
    2. Reasonably related to CMU's costs of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged;
    3. 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
    4. Based on costs not otherwise recovered for the same instance of service to a provider and third party.

b. The fees CMU charges must not be based on:
    1. Whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with CMU;
    2. 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;
    3. Costs CMU 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;
    4. Costs associated with intangible assets others than the actual development or acquisition costs of such assets;
    5. Opportunity costs unrelated to the access, exchange, or use of the EHI; or
    6. Any costs that led to the creation of intellectual property, if CMU charged a royalty for the intellectual property pursuant to the Licensing Exception and that royalty included the development costs for creation of the intellectual property.

c. Excluded fees condition. This exception does not apply to:
    1. A fee prohibited by the HIPAA Privacy Rule;
    2. A fee based in any part on the electronic Access of an individual's EHI by the individual, the individual's legal 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 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.

d. Comply with Conditions of Certification in § 170.402(a)(4) (Assurances – certification to "EHI Export" criterion) or 45 CFR § 170.404 (API).

XI. Licensing exception: It will not be information blocking for CMU to license interoperability elements for EHI to be accessed, exchanged, or used, provided the below conditions are met:

a. The practice must meet:

1. The negotiating a license conditions: CMU must begin license negotiations with the requestor within 10 business days from receipt of the request and negotiate a license within 30 business days from receipt of the request.
2. The licensing conditions:
   i. Scope of rights
   ii. Reasonable royalty
   iii. Non-discriminatory terms
   iv. Collateral terms
   v. Non-disclosure agreement
   vi. Additional conditions relating to the provision of interoperability elements.

XII. Documentation Requirement:

a. When utilizing any of the above exceptions, workforce members are required to document use of the exception and provide documentation to the applicable department representative for retention.

Central Michigan University reserves the right to make exceptions to modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines related to this subject.