Clark County, Wisconsin
Title: Information Blocking Policy

Title: Information Blocking Policy	**Effective Date:** April 5, 2021
	Adoption/Revision Date: April 5, 2021
Custodian: County Attorney	**Approving Body:** Clark County Board of Supervisors

1. **Authority**
    a. Wis. Stat. 59.02, 59.03, 59.51, 59.52, 42 U.S.C. 300, and 45 C.F.R. 171
2. **References**
    a. Adopting Resolution/Ordinance/Motion: Resolution 52-12-13
    b. Clark County HIPAA Policies and Forms
    c. Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
    d. 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule
3. **Purpose/Policy Overview**
    a. To establish processes and guidelines to facilitate and support the timely access, exchange, and use of electronic health information.
    b. Clark County is committed to making electronic health information available and usable for authorized and permitted purposes available by applicable laws.
    c. This policy assists in deterring the information blocking often faced by Covered Functions when attempting to provide informed healthcare to clients.
4. **Scope**
    a. This policy applies to the access, exchange, and use of electronic health information for all Clark County Covered Functions. In the event any policy violates federal or state law or is held invalid by a court of competent jurisdiction, the affected policy shall be deemed to have been severed from this policy to the extent of its invalidity.
5. **Definitions**
    a. The terms below have the following meanings in this policy:
        i. Designated record set means medical records, billing records, or any other group of records maintained by or for a covered function to make decisions about individuals.
        ii. Electronic health information (EHI) means any individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by electronic media by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations that are contained in a designated record set.
            1. EHI does not include psychotherapy notes, which are notes created and recorded by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
        iii. Final Rule means 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule.
        iv. Covered Functions mean Clark County department and functions identified to be covered function under Clark County's HIPAA Applicability Policy.

v. Interoperability elements means hardware, software, integrated technologies or related licenses, technical information, privileges, rights, intellectual property, upgrades, or services that may be necessary to access, exchange, and/or use of EHI that are controlled by Clark County, which includes the ability to confer all rights and authorizations necessary to use the element to enable the access, exchange, and/or use of EHI.

6. **General**
    a. The Final Rules prohibits Covered Functions from engaging in practices that are likely to interfere with the access, exchange, and/or use of EHI unless the practice is required by law or the practice is permissible as an exception as identified in this policy.
        i. The Final Rule does not require Covered Functions to disclose EHI if disclosure would violate other applicable laws (i.e. HIPAA).
7. **General**
    a. The Final Rule sets forth eight (8) practices, or Safe Harbors, that do not constitute information blocking even if the practice does interfere with the access, exchange, or use of EHI. Safe Harbors are determined to be practices, or exceptions to disclosure, that are reasonable and necessary to further the Final Rule's intent.
    b. For a Safe Harbor to apply, all elements for each specific exception shall be met. Further, more than one (1) Safe Harbor may apply.
    c. The interference with the access, exchange, and/or use of EHI that does not meet the elements of a specific exception may not constitute information blocking and will be analyzed on a case-by-case basis.
    d. The following are the eight (8) Safe Harbors: 1) Preventing Harm; 2) Privacy; 3) Security; 4) Content and Manner; 5) Infeasibility; 6) Fees; 7) Licensing; and 8) IT Performance. Each Safe Harbor is set forth below with a citation to the federal code for further information.
    e. Covered Functions shall adhere to HIPAA accessibility policies/practices when 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.
8. **Safe Harbor – Preventing Harm (45 C.F.R. 171.201)**
    a. If conditions of the Preventing Harm Safe Harbor are met, information blocking does not occur if a practice substantially reduces a reasonable cognizable risk of harm to a natural person.
    b. For requestors other than an individual or legal representative, Covered Functions may delay, deny, or otherwise interfere with the requestor's access, exchange, and/or use of EHI if there is 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:
        i. 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
        ii. 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.

c. If either circumstance applies, the practice shall not be 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 the interference with the access, exchange, and/or use of EHI. If this practice is relied upon, the individual who makes the risk of harm determination will document this determination and retain such documentation accordingly. If it is appropriate to do so, this documentation may be kept in the affected individual's medical record.

9. **Safe Harbor – Privacy (45 C.F.R. 171.202)**
    a. If conditions of the Privacy Safe Harbor are met, information blocking does not occur if a practice protects the privacy of the EHI subject.
    b. Covered Functions shall adhere to HIPAA accessibility policies/practices with respect to granting, delaying or denying a third-party's request for access, exchange, and/or use of EHI, including when a legal precondition must be met. Practices shall be 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 include, but are not limited to, written, informed consent or release of information or verification of identity and authority.
    c. Covered Functions may elect to not provide access, exchange, and/or use of EHI if the following conditions are met:
        i. The individual, who is the subject of the EHI, requests to not provide such access, exchange, and/or use of the individual's EHI.
        ii. Documentation of the request shall be made within a reasonable time period after the request is made.
        iii. The practice of granting an individual's request not to share EHI in a consistent and non-discriminatory manner.
        iv. An individual's request for a restriction only under one of the following circumstances:
            1. The individual agrees to the termination in writing or requests the termination in writing;
            2. The individual orally agrees to the termination and the communication is documented; or
            3. Covered function notifies the individual that it is terminating its agreement except that such termination is not effective to the extent prohibited by other applicable laws and only applies to EHI created or received after the individual is informed of the termination.

10. **Safe Harbor – Security (45 C.F.R. 171.203)**
    a. If conditions of the Security Safe Harbor are met, information blocking does not occur if a practice protects the security of the EHI.
    b. Covered Functions shall adhere to HIPAA accessibility policies/practices with respect to granting, delaying, denying or otherwise interfering with the provision of access, exchange, and/or use of EHI. Security practices shall be:
        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 across similarly situated persons or entities whose interactions pose the same level of security risk.

c. In the event Clark County's HIPAA security policies and procedures do not sufficiently address a known security risk, the individual who makes the security risk determination shall document the security practice based on particularized facts and circumstances surrounding the security risk, including:
    i. Why the security practice was necessary to mitigate the security risk to EHI; and
    ii. That there were no reasonable and appropriate alternative that would address the security risk and would be less likely to interfere with the access, exchange, and/or use of EHI.
        1. This last factor will be highly dependent on the urgency and nature of the security threat in question. In the event of exigent circumstances, the individual 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, and/or use of EHI. However, the initial-response practice may be in place for only a short time and contingent upon more fully identifying and assessing current risks in context or as follow-up to the exigent circumstances. If appropriate, the individual shall modify or replace its initial-response practice with a less onerous alternative that is reasonable and appropriately tailored to the specific risk addressed.

d. Covered Functions may (but are 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, and/or use of EHI so long as all three of the following requirements are met:
    i. The information focuses on current privacy and/or security risks of the technology or the third-party developer;
    ii. The information is factually accurate, unbiased, objective, and is not unfair or deceptive; and
    iii. The information is provided in a non-discriminatory manner.

e. Covered Functions may provide this education through an automated attestation and warning process upon request from an individual to transmit data to a third-party application. Clark County 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.

f. Security practices shall not be engaged in that have the practical effect of disadvantaging competitors or steering referrals.

11. **Safe Harbor – Content and Manner (45 C.F.R. 171.301)**

a. If conditions of the Content and Manner Safe Harbor are met, information blocking does not occur if a Covered Function fulfills a request for EHI in an alternative manner than the one requested.

b. A response to an EHI request may be made in an alternative manner if one of the following circumstances applies:
    i. The request cannot be fulfilled as requested due to technical limitations; or
    ii. Parties cannot agree on terms for access, exchange, and/or use of EHI.

c. If the Covered Function is technically unable to fulfill the request in the manner requested or cannot reach agreeable terms with the requestor, the request shall be

fulfilled in an alternative manner and without unnecessary delay unless it is infeasible to do so.

d. The requestor shall be notified within ten (10) business days of the request if fulfilling the EHI request in the manner requested or in an alternative manner is infeasible.
e. If responding in an alternative manner is feasible, the request shall be technically fulfilled using the technical standards listed below in the following order of priority, only proceeding to the next technical standard if technically unable to fulfill the request using the higher priority standard:
    i. Using certified technology specified by the requestor (i.e. application programming interface (API), direct protocol); or
    ii. 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
    iii. Using an alternative machine-readable format agreed upon with the requestor (i.e. Portable Document Format (PDF), comma-separated value (CSV) files).
f. Covered Functions 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.

12. **Safe Harbor – Infeasibility (45 C.F.R. 171.204)**
    a. If conditions of the Infeasibility Safe Harbor are met, information blocking does not occur if a Covered Function faces legitimate practical challenges that limit the ability to comply with the request for access, exchange, and/or use of EHI.
    b. If an individual makes an infeasibility determination for any of the three (3) reasons stated below, the requestor shall be notified of the infeasibility determination in writing including the reason(s) for the infeasibility determination within ten (10) business days of the EHI request. A request for EHI may be infeasible to comply with if any of the following applies:
        i. 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.
        ii. Requested EHI cannot unambiguously be separated from the EHI that cannot be disclosed due to an individual's privacy preferences or legal requirements.
        iii. The following factors make complying with the EHI request infeasible:
            1. The type of EHI and the purposes for which it may be needed;
            2. The cost of complying with the request in the manner requested;
            3. The financial and technical resources;
            4. Practice is nondiscriminatory in its application to others;
            5. Ownership or control over predominant technology or platform through which the EHI can be accessed or exchanged; and
            6. Why the EHI could not be made available through an alternative manner.
    c. In making such a determination, the following factors may not be considered:
        i. Whether complying with the EHI request in the manner requested would facilitate competition; and
        ii. Whether complying with the EHI request would prevent charging a fee or will

result in a reduced fee.

d. Documentation of the analysis of factors shall be created and maintained. Factors shall be analyzed consistently and in a non-discriminatory manner.

13. **Safe Harbor – Fees (45 C.F.R. 171.302)**
    a. If conditions of the Fees Safe Harbor are met, information blocking does not occur if a Covered Function fulfills a request for EHI in an alternative manner than the one requested and charges a reasonable fee. The Fees Safe Harbor does not permit or support the sale of EHI.
    b. Covered Functions shall adhere to HIPAA accessibility policies/practices related to any fees charged to an individual's (or personal representative's) request to access the individual's EHI. Fees shall not be charged 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, fees will not be charged for electronic access if an individual directs 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.
    c. For requestors other than an individual or personal representative, a fee may be charged (but is not required to) for the access, exchange, and/or use of EHI as long as the fee is based on the following:
        i. Objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;
        ii. Reasonably related to actual costs of providing the type of access, exchange, and/or use of EHI 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. Costs not otherwise recovered for the same instance of service to a provider and third-party.
    d. Any fees charged will not be based on any of the following (if applicable):
        i. Whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition;
        ii. Sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, and/or use of EHI;
        iii. Costs 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, and/or use the EHI;
        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, and/or use of EHI;
        vi. Any costs that led to the creation of intellectual property if a royalty is charged for that intellectual property and that royalty included the development costs for the creation of the intellectual property; or
        vii. 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 EHI technology that was not agreed to in writing at the time the technology was acquired.

14. **Safe Harbor – Licensing (45 C.F.R. 171.303)**
    a. If conditions of the Licensing Safe Harbor are met, information blocking does not occur if a Covered Function fulfills a request for EHI in an alternative manner than the one requested and imposes terms and conditions (i.e. a license or non-disclosure agreement) on the requestor's use of Interoperability Elements to access, exchange, and/or use of EHI.
    b. In the event Organization licenses the use of Interoperability Elements to access, exchange, and/or use EHI in an alternative manner, the following process shall be followed:
        i. Begin license negotiations with a requestor within ten (10) business days of the request; and
        ii. Negotiate in good faith a license within thirty (30) business days of the request.
    c. The license will meet all of the following requirements (as applicable):
        i. The scope of the license will provide all rights necessary to enable the access, exchange, and/or use of EHI to achieve the intended access, exchange, and/or use of EHI via the Interoperability Elements.
        ii. If a royalty is charged, the royalty will be reasonable, non-discriminatory and based solely on the independent value of the technology to the licensee's products. A royalty will not be based on any strategic value stemming from control over essential means of accessing, exchanging, and/or using EHI. If the Interoperability Elements are licensed through a standards developing organization, a royalty may be charged that is consistent with such policies. A royalty shall not be charged for intellectual property if any development costs are recovered that led to the creation of the intellectual property.

15. **Safe Harbor – IT Performance (45 C.F.R. 171.205)**
    a. If the conditions of the IT Performance Safe Harbor are met, information blocking does not occur if the practice is necessary to maintain and/or improve the health IT performance.
    b. If IT related to the access, exchange, and/or use of EHI that is under Clark County's control is temporarily unavailable, or temporarily degrades the performance of health IT, in order to perform maintenance or improvements to the health IT, the practice must be:
        i. 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;
        ii. Implemented in a consistent and non-discriminatory manner; and
        iii. If the unavailability or degradation is initiated by a health IT developer of certified health IT, health information exchange, or health information network:
            1. Consistent with existing service level agreements between the individual or entity to whom the health IT developer of certified health IT, health information exchange, or health information network supplied the health IT; or
            2. 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, health information exchange, or health information network supplied the health IT.

c. Action against a third-party application that is negatively impacting the health IT's performance may be executed provided that the practice meets all the following:
    i. For a period of time no longer than necessary to resolve any negative impacts;
    ii. Implemented in a consistent and non-discriminatory manner; and
    iii. Consistent with existing service level agreements, where applicable.

16. **Reporting**
    a. Employees that reasonably believe that a violation of this policy has occurred shall immediately report the alleged violation to their respective department head. The department head shall report the alleged violation to the Privacy Officer as soon as practical.
    b. The Privacy Officer shall respond to all reported violations and complete an investigation if deemed appropriate.
    c. Clark County shall not retaliate against any employee for reporting a suspected violation of this policy or the Final Rule.
17. **Training and Compliance**
    a. All employees of Covered Functions shall be trained on this policy on a periodic and ongoing basis. Evidence of training shall be documented and retained.
    b. Questions about this policy shall be directed to the Privacy Officer.
    c. Compliance and training/education are an ongoing process and any compliance issues will be addressed as they arise. Violations of this policy may result in discipline including, but not limited to, termination.

Revision History		
Adoption/Revision Date	**Overview of Adoption/Revision**	**Adoption/Revision Reference**
April 5, 2021	New policy to information blocking	Resolution 52-12-13