# HIPAA PRIVACY POLICY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended from time to time, including by the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), grants individuals the right to receive notice of the uses and disclosures of their Protected Health Information that may be made by the Participating Member in The Jefferson Health Plan (the Plan, fka the OME-RESA Health Benefits Program) on behalf of the Plan and sets forth the individual's rights and the Participating Member's legal obligations with respect to Protected Health Information. The purpose of this policy is to assist the Participating Member in complying with the HIPAA privacy standards, to ensure that individuals receive adequate notice of the Participating Member's practices with regard to the dissemination and use of Protected Health Information, and to protect the confidentiality and integrity of Protected Health Information.

## Definitions

For the purposes of this policy, the following definitions shall apply:

Individually Identifiable Health Information is a subset of health information, including demographic information collected from an individual and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information or PHI is Individually Identifiable Health Information that is transmitted by electronic means; maintained in any electronic medium, such as magnetic tape, disc, or optical file; or transmitted or maintained in any other form or medium, such as paper, verbal, email, or fax.

Covered Functions are those functions of the Plan's Participating Member, the performance of which, makes the Participating Member a health plan, health care provider, or health care clearinghouse.

Designated Record Set is a group of records maintained by or for the Participating Member that is medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan; or used in whole or in part by or for the Plan and/or the Participating Member to make decisions about individuals.

Business Associate is a person or entity that provides certain functions, activities, or services for or on behalf of the Plan and/or the Participating Member involving the use and/or disclosure of Protected Health Information.

Participating Member is a political subdivision of the State of Ohio that participates in the Plan.

Plan is a regional council of governments formed pursuant to Ohio Revised Code Chapter 167 to provide a partially self-funded benefit program for any political subdivision wishing to provide health care and related benefits to employees and dependents covered under the Member's benefit plans and whose governing body has authorized participation in the Plan.

**Confidentiality of Individually Identifiable Health Information**

All officers, employees, and agents of the Participating Member shall preserve the confidentiality and integrity of Individually Identifiable Health Information pertaining to any individual. Individually Identifiable Health Information is Protected Health Information and shall be safeguarded to the extent possible in compliance with the requirements of the security and privacy rules and standards established by HIPAA.

The Participating Member and its officers, employees, and agents will not use or disclose an individual's PHI for any purpose without the properly documented consent or authorization of the individual or his/her authorized representative unless required or authorized to do so under state or federal law or this policy, unless an emergency exists, or unless the information has been sufficiently de-identified that the recipient of the information would be unable to link the information to a specific individual. All uses or disclosures of PHI will be limited to the minimum amount necessary to accomplish the stated purpose or will be in conformity with such other restrictions as the Participating Member may have agreed to.

All officers, employees, and agents of the Participating Member are expected to comply with and cooperate fully with the administration of this policy. The Participating Member will not tolerate any violation of the HIPAA privacy or security standards or this policy. Any such violation shall constitute grounds for disciplinary action up to and including termination of employment.

Any officer, employee, or agent of any Participating Member who believes that there has been a breach of these privacy and security policies and procedures or a breach of the integrity or confidentiality of any person's PHI shall immediately report such breach to his or her immediate supervisor or the formally appointed Privacy Officer. The Privacy Officer shall conduct a thorough and confidential investigation of any reported breach and notify the complainant of the results of the investigation and any corrective action taken.

The Participating Member will not retaliate or permit reprisals against any employee who reports a breach to the integrity or confidentiality of PHI. Any employee involved in retaliatory behavior or reprisals against another individual for reporting an infraction of this policy shall be subject to disciplinary action up to and including termination of employment.

**Security Provisions**

The Participating Member shall take reasonable steps to limit the use and/or disclosure of and requests for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request and to determine the extent to which various classifications of employees

need access to such information. The Participating Member shall also implement reasonable administrative, technical, and physical safeguards to protect Individually Identifiable Health Information from any intentional or unintentional use or disclosure and that mitigate, to the extent practicable, any harmful effect that is known to the Participating Member as a result of a use or disclosure of PHI in violation of this policy or the HIPAA privacy and security standards. The Participating Member's security measures shall include the following:

A. Administrative procedures to guard data integrity, confidentiality, and availability, including documented, formal practices to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to the protection of data;

B. Physical safeguards to protect data integrity, confidentiality, and availability including the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards and from intrusion and the use of locks, keys, and other administrative measures to control access to computer systems and facilities;

C. Technical security services to protect data integrity, confidentiality, and availability including processes put in place to protect information and to control individual access to information;

D. Technical security mechanisms including processes put in place to protect against unauthorized access to data that is transmitted over a communications network; and

E. The optional use of an electronic digital signature.

**Mitigating the Effects of Unauthorized Use or Disclosure**

If the Privacy Officer determines that there has been a breach of this privacy policy or the procedures of the Participating Member, he/she shall make a determination of the potential harmful effects of the unauthorized use or disclosure and decide upon a course of action to minimize the harm. Any individual responsible for the unauthorized use or disclosure shall be referred to the Participating Member's designee for appropriate disciplinary action and additional training, if applicable.

If the Privacy Officer or a Business Associate determines that there has been a breach of unsecured PHI, as defined in the HITECH Act, the Participating Member and/or the Business Associate shall provide the required breach notifications to impacted individuals, the media and the Secretary of Health and Human Services, as necessary and required.

**Use or Disclosure of Protected Health Information**

The Participating Member may use and disclose PHI, without the written consent of the individual or his/her authorized representative, both within and outside of the Participating Member's jurisdiction, for the following purposes:

A. Treatment: The provision, coordination, or management of health care, health care services or supplies related to an individual and related services by or among providers, providers and third parties, and referrals from one provider to another.

B. Payment: Activities undertaken by a health plan to obtain premiums or determine responsibility for coverage, or activities of a health care provider or health plan to obtain reimbursement for the provision of health care. Payment activities include, but are not limited to, billing, claims management, collection activities, eligibility determination, and utilization review.

C. Health Care Operations: Activities of the Plan and/or the Participating Member to the extent such activities are related to Covered Functions including quality assessment and improvement activities; credentialing health care professionals; insurance rating and other insurance activities related to the creation or renewal of a contract for insurance (provided, however, that if PHI is disclosed for underwriting purposes, no genetic information will be used or disclosed for this purpose); conducting or arranging for medical review, legal services and auditing functions, including compliance programs; business planning such as conducting cost-management and planning analyses to managing and operating the Participating Member including formulary development and administration, development, improvements for methods of payment or coverage policies; business management and general administration activities; due diligence in connection with the sale or transfer of assets to a potential successor in interest if the potential successor is a covered entity or will become a covered entity; consistent with privacy requirements, creating de-identified health information, fundraising for the benefit of the covered entity and marketing for which an individual authorization is not required.

D. As required by, or to comply with, law.

E. For public health and safety activities.

F. About victims of abuse, neglect, or domestic violence.

G. To health oversight agencies in connection with health oversight activities.

H. For judicial and administrative proceedings, or to comply with a lawfully issued subpoena.

I. For law enforcement purposes.

J. Regarding decedents to coroners, medical examiners, and funeral directors.

K. For research if a waiver of authorization has been obtained.

L. To prevent serious and imminent harm to the health or safety of a person or the public.

M. For specialized governmental functions.

N. Military and veterans' activities.

O. National security and intelligence.

P. Protective services for the President and others.

Q. To the Department of the State to make medical suitability determinations.

R. To correctional institutions and law enforcement officials regarding an inmate.

S. Workers' compensation if necessary to comply with the laws relating to workers' compensation and other similar programs.

T. To Business Associates for the purpose of assisting the Participating Member in completing healthcare functions.

Prior to releasing any PHI for the purposes set forth above, the Participating Member's representative disclosing the information shall verify the identity and authority of the individual to whom disclosure is made. This verification may include the examination of official documents, badges, driver's licenses, workplace identity cards, credentials, or other relevant forms of identification or verification.

**Authorization**

The Participating Member shall not disclose PHI for purposes other than those set forth above without a valid authorization. A valid authorization is a document signed by the individual that gives the Plan and/or Participating Member permission to use specified health information for a specified purpose and time frame. The Participating Member shall not condition the provision of treatment, payment, enrollment in the Plan, or eligibility for benefits on an individual's provision of authorization except:

A. The Participating Member may condition the provision of research-related treatment on the provision of an authorization.

B. The Plan may condition enrollment or eligibility for benefits on the provision of an authorization requested by the Plan prior to enrollment.

C. The authorization is sought for the Plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations.

D. The Participating Member may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization for the disclosure of the PHI to the third party.

To be valid, an authorization shall contain at least the following elements:

A. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

B. The name or other specific identification of the person(s) or class of person(s) authorized to make the requested use or disclosure;

C. The name or other specific identification of the person(s) or class of person(s) to whom the Plan and/or the Participating Member may make the requested use or disclosure;

D. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

E. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke together with a description of how the individual may revoke the authorization;

F. A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule; and

G. Signature of the individual and date and, if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

In addition to the requirements set forth above, an authorization requested by the Plan and/or the Participating Member for its own use of the PHI that it maintains, must comply with the following additional requirements:

A. A statement that the Plan and/ or the Participating Member will not condition treatment, payment, enrollment in the Plan, or eligibility for benefits upon the individual's provision of authorization for the requested use;

B. A description of each purpose of the requested use or disclosure;

C. A statement that the individual may inspect or copy the PHI to be used or disclosed and refuse to sign the authorization; and

D. If the disclosure of the requested information will result in direct or indirect remuneration to the Plan and/or the Participating Member from a third party, a statement that remuneration will result.

The Plan and/or the Participating Member shall provide the individual with a copy of the signed authorization.

An authorization for the use or disclosure of PHI may not be combined with any other document to create a compound authorization.

An authorization is not valid if the document submitted has any of the following defects:

A. The expiration date has passed or the expiration event is known to have occurred;

B. Any required element is missing or has not been filled out;

C. The authorization is known to have been revoked;

D. The authorization has been improperly combined with another document;

E. The Plan and/or the Participating Member has violated the rules on making the authorization a condition; or

F. Any material information in the authorization is known to be false.

An individual may revoke an authorization at any time, provided the revocation is in writing.

**Rights Related to Protected Health Information**

Individuals shall have the following rights with regard to their PHI:

A. Access. Individuals shall have the right to access their own PHI that is maintained in a Designated Record Set of the Plan, the Participating Member and its Business Associates.

B. Restrictions. Individuals shall have the right to request restrictions on how the Participating Member will use or disclose the individual's own PHI for treatment, payment or health care operations and how the individual's information will be disclosed or not disclosed to family members or others involved in the individual's care. The Participating Member shall comply with the individual's reasonable request to receive communications of PHI by alternative means or at alternative locations.

C. Amendment. Individuals shall have the right to amend erroneous or incomplete PHI unless the information:

1. Was not created by the Participating Member;

2. Is not in a Designated Record Set or is not otherwise available for inspection;

3. Is accurate and complete; or

4. Is not subject to the right of access.

A request to amend PHI must be submitted to the Privacy Officer in writing. The Privacy Officer shall review the request and respond in writing within thirty calendar days. If a request to amend is denied, the individual may appeal the denial using the complaint procedure set forth in this policy. The denial must be written in plain language and contain:

- The basis for the denial;
- A statement of the individual's right to submit a written statement disagreeing with the denial and how it may be filed;
- A statement that if the individual does not submit a statement of disagreement, his/her right to request that the request for amendment and its denial be provided with any future disclosure of the PHI that is the subject of the request for amendment;
- A description of how the individual may appeal the denial; and
- The right of the Participating Member to reasonably limit the length of the statement of disagreement.

The Participating Member may also choose to prepare a written rebuttal to the statement of disagreement and provide a copy to the individual. All of the statements related to the amendment denial shall become part of the individual's Designated Record Set and shall be linked to the individual's PHI.

D. Accounting. Individuals shall have the right to an accounting of disclosures of their own PHI that is maintained in a Designated Record Set of the Participating Member and its Business Associates. Such accounting can include a period of six years prior to the request.

The Plan and/or the Participating Member may adopt corresponding policies and procedures, including necessary forms, to implement and administer these participant rights.

**Business Associates**

The Participating Member, its officers, employees, and agents shall not disclose PHI to any Business Associate in the absence of a written contract with the Business Associate that assures that the Business Associate will use the information only for the purposes for which it was engaged by the Participating Member; will safeguard the information from misuse; and will assist the Participating Member in complying with its duties to provide individuals with access to health information about them and a history of certain disclosures. The Participating Member shall disclose PHI to a Business Associate for the sole purpose of assisting the Participating Member in completing healthcare functions, not for the independent use by the Business Associate.

The Participating Member shall enter into a contract with each Business Associate, which shall be a document separate from the service agreement, if any. The Privacy Officer shall be responsible for managing all Business Associate contracts and ensuring that they are current and in compliance with the requirements of this policy and HIPAA. Under the contract, the Business Associate shall be obligated to notify the Privacy Officer when unauthorized uses and/or disclosures of PHI have occurred in the Business Associate's organization or by a subcontractor of the Business Associate. The Privacy Officer will take appropriate steps to address the violation up to and including termination of the business associate contract.

However, the Participating Member shall not be liable for privacy violations of a Business Associate or its subcontractors, if any, and the Participating Member is not required to actively monitor or oversee the means by which a Business Associate carries out safeguards or the extent to which a Business Associate abides by the requirements of the contract.

The contract between the Participating Member and the Business Associate shall further obligate the Business Associate to enter into a written agreement with any subcontractor. Such agreement shall require the subcontractor to comply with the same restrictions and conditions that apply to the Business Associate with respect to protected health information and require the Business Associate to take appropriate steps to address any unauthorized uses and/or disclosures of PHI by the subcontractor up to and including termination of the agreement with the subcontractor.

**Privacy Officer**

Unless otherwise appointed in writing, the Treasurer, Fiscal Agent or Human Resources Designee shall be the Privacy Officer for the Participating Member. The Privacy Officer will be responsible for overseeing all ongoing activities related to the development, implementation, maintenance, and adherence to the Participating Member's policies and procedures concerning the security and privacy of PHI.

**Complaint Procedure**

The following procedure shall be used for the processing of complaints regarding the collection, use, management, disclosure, or amendment of PHI:

Step 1 – A written complaint must be submitted to the Privacy Officer. A complaint can also be made directly to the Secretary of Health and Human Services. Upon receipt of a complaint, the Privacy Officer will review the complaint, conduct any necessary investigation, and provide the complainant with a written disposition within ten working days.

Step 2 – The disposition of the Privacy Officer may be appealed by the complainant to the Participating Member's designee within ten working days of receipt of the disposition of the Privacy Officer. The Participating Member's designee shall meet within ten working days with the complainant, the Privacy Officer, and any other necessary individuals. The Participating Member's designee will respond in writing to the complainant within ten working days following the meeting.

Step 3 – If the complaint is not satisfactorily resolved, a written appeal may be made to the Participating Member's board or governing body within ten working days of receipt of the Participating Member's designee's decision. The board or governing body will meet with the complainant at its next regular meeting and provide a written response to the complaint no later than the following regular meeting.

**Notice of Privacy Practices**

The Participating Member shall distribute a Notice of Privacy Practices to individuals at the time of their enrollment in the Plan and within sixty days of any material revision. The notice shall also be posted in a clear and prominent location in each facility of the Participating Member and be available electronically and/or printed in staff handbooks and the health plan booklet. The Participating Member will also notify individuals covered by the Plan of the availability of and how to obtain the notice at least once every three years. The notice shall adequately inform individuals of their rights to:

A. Request restrictions on certain uses and disclosures of PHI;

B. Request the communication of confidential information by some reasonable alternative means or at an alternative location;

C. Inspect and copy records or receive a summary of specific information;

D. Request that PHI be amended;

E. Request an accounting of certain disclosures of PHI; and

F. Receive a paper copy of the notice upon request.

**Training**

All employees and Business Associates shall receive training regarding the Participating Member's privacy policies and procedures as necessary and appropriate to carry out their job duties as they may relate to the administration of the Plan. Training shall also be provided when there is a material change in the Participating Member's privacy practices or procedures.

**Documentation**

Documentation shall be maintained in support of the policies and procedures of the Participating Member, consistent with the parts of HIPAA's privacy regulations that directly require documentation, including, but not limited to, all authorizations and revocations of authorizations and complaints and disposition of complaints. All documentation shall be kept in written or electronic form for a period of six years from the date of creation or from the date when it was last in effect, whichever is later.