PIPE FITTERS LOCAL UNION NO. 211
WELFARE TRUST
FUND
HIPAA Policy and Procedure Manual

Effective: January 1, 2026

This HIPAA Policy and Procedure Manual is adopted and established by the Pipe Fitters Local Union No. 211 Welfare Trust Fund's, group health plan(s), the "Plan" or "Group Health Plan".

This manual includes provisions to assist the Plan in complying with the HIPAA Final Rule issued by the U. S. Department of Health and Human Services, modifying the Privacy, Security, Breach Notification and Enforcement Rules under the Health Insurance Portability and Accountability Act (HIPAA) published in the January 25, 2013 Federal Register, titled: *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Genetic Information Nondiscrimination Act (GINA); Other Modifications to the HIPAA Rules*.

The Plan has no employees and, while the Plan Sponsor is entitled to receive Protected Health Information ("PHI"), in general, the information is required to be de-identified before it is sent to the Plan Sponsor. If de-identification is not practical, minimum necessary information is sent in **non-electronic** media such as fax, mail, messenger or phone.

The Plan's functions, including creation and maintenance of its records, are mainly carried out by the Business Associates of the Plan. Neither the Plan nor the Plan Sponsor own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by Business Associates. Accordingly, the Business Associates create, receive, maintain, and transmit all PHI and electronic PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit PHI and electronic PHI relating to the Plan, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Plan will request appropriate changes from the Business Associate if they become aware of any potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI relating to the Plan. That responsibility lies solely with the Plan's Business Associates.

Recognizing that the main burden of safeguarding PHI, including electronic PHI is on its Business Associates, the Plan Sponsor on behalf of the Plan has contracted with Business Associates to require that such Business Associates undertake certain obligations relating to the security of PHI and electronic PHI that they handle in relation to the performance of administrative functions for the Plan. The Plan will receive from each of its Business Associates, a Business Associate Agreement meeting the requirements of the HIPAA Final Rules and, upon request:

1) Verify that the Business Associate has adopted HIPAA policies and procedures in compliance with the HIPAA Final Rules;

2) Confirm, in writing, that it is in full compliance with the Business Associate Agreement and applicable HIPAA Final Rules.

As it relates specifically to the Security Rules, HIPAA, HITECH and their implementing regulations and guidance require the Plan to implement various security measures with respect to electronic PHI. As previously stated, the Plan has no employees and, while the Plan Sponsor is entitled to receive PHI, in general, the information is required to be de-identified before it is sent to the Plan Sponsor in a non-electronic format.

Neither the Plan nor the Plan Sponsor have access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Business Associates affecting the security of the Plan's electronic PHI. Therefore, the Plan's HIPAA policies and procedures, do not separately address the following standards (including the implementation specifications associated with them):

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

DEFINITIONS:

Throughout these policies and procedures, the following terms are used liberally and defined below:

Administrative Office means Benefit Resources, Inc. (the contracted third party administrator) whose role is to administer the terms of the Plan.

Business Associate means, with respect to a Covered Entity, a person who: (i) on behalf of such Covered Entity, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (ii) provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501), management, administrative, accreditation, or financial services to or for such Covered Entity, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

Covered Entity means a health plan, health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by

the HIPAA Rules. As it relates to these HIPAA Policies and Procedures, the Fund's self-funded Group Health Plan is the Covered Entity.

Fund means Pipe Fitters Local Union No. 211 Welfare Trust Fund.

Plan or Group Health Plan means the self-funded components of the Fund's Group Health Plan. For purposes of this HIPAA Policy and Procedure Manual, the Plan does not include any fully-insured health plans.

Protected Health Information "PHI" means information that is created or received by or on behalf of the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased.

Protected health information (PHI) does <u>not</u> include individually identifiable health information in:

- Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
- Records described at 20 U.S.C. 1232g(a)(4)(B)(iv) (FERPA records on students 18 and over); and
- Employment records held by a Covered Entity (e.g. the "Plan") in its role as an employer such as records maintained in compliance with OSHA, Family and Medical Leave Act (FMLA), workers' compensation, and alcohol and drug free workplace laws, and
- Reference to a person who has been deceased for more than 50 years.

Electronic PHI means PHI that is transmitted by or maintained in electronic media or transmitted or maintained in any other form or medium by or on behalf of a Covered Entity.

- **Electronic Media means**:
  - Electronic storage material on which data is or may be recorded electronically, including devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
  - Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, voice via telephone, and facsimile, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Plan Sponsor means the Board of Trustees of the Fund's Group Health Plan.

Privacy & Security Officer means the Privacy and Security Officer who has been designated as the Privacy & Security Officer on behalf of the Plan. Questions or comments about the policies and procedures in this manual should be referred to Cory Crandell, the Plan's Privacy and Security Officer at:

c/o Benefit Resources, Inc.
8441 Gulf Freeway, Suite 304
Houston, TX 77017
Telephone: (713) 643-9300
Fax #: (866) 316-4794

Workforce Member means HIPAA regulated employees, Trustees, volunteers, trainees, and other persons whose performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.

It is the Plan's policy to comply fully with the requirements of the HIPAA Rules. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), the Plan will follow the revised rules.

The Plan reserves the right to amend or change these policies and procedures at any time (and even retroactively) without notice. To the extent that these policies and procedures establish requirements and obligations above and beyond those required by HIPAA, the policies and procedures shall be aspirational and shall not be binding upon the Plan.

Table of Contents

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section § 164.520 of the HIPAA Rules and 42 CFR 2.22. and their implementing regulations and guidance. If these Rules are changed by the Department of Health and Human Services (HHS), the Plan will follow the revised rules.

An individual has the right to adequate notice of the Uses and Disclosure of PHI that may be made by the Plan, the rights of the individual and the legal duties of the Plan with respect to PHI. In addition, as provided in 42 CFR 2.22, an individual who is the subject of records protected under 42 CFR Part 2, has a right to adequate notice of the uses and disclosures of such records, and of the individual's rights and the Covered Entity's legal duties with respect to such records.

A. **Privacy Notice Distribution**: The initial distribution of the Privacy Notice occurred on or before April 14, 2003. Thereafter, the Privacy Notice will be provided to the "Named Insured" covered under the Plan at the following times:

- To all new enrollees at the time of enrollment,
- Upon any Material Revisions, the Plan will either:
  - If a website exists for the Plan, the Plan will prominently display the Privacy Notice on its website by the effective date of the Material Revision to the Privacy Notice. Additionally, the Plan will provide the revised Privacy Notice or information about the Material Revision and how to obtain the revised Privacy Notice, in its next annual mailing to individuals then covered by the Plan; or
  - If the Plan does not maintain a website or the Privacy Notice is not posted on its website by the effective date of the Material Revision, the Plan will provide the revised Privacy Notice, or information about the Material Revision and how to obtain the revised Privacy Notice, to individuals then covered by the Plan within 60 days of the Material Revision to the Privacy Notice.
- Upon request.

B. **Privacy Notice Reminders**: No less frequently than once every three years, individuals then covered by the Plan will be notified of the availability of the Privacy Notice and how to obtain the Privacy Notice.

C. In compliance with 164.530 (i) and 502(i) neither the Plan nor the Plan Sponsor will use or disclose PHI in a manner inconsistent with the Privacy Notice.

D. **Privacy Notice Content**: The content of the Privacy Notice will comply with the requirements of the HIPAA Privacy regulation at 164.520 (b). It will:

- include the following required header text:
  - "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

- address uses and disclosures including at least one example of the types of uses and disclosures the Plan makes for treatment, payment and healthcare operations ("TPO"),

- a description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

- if a use or disclosure for any purpose described in the two prior bullets is prohibited or materially limited by other applicable law, such as 42 CFR Part 2 (addressing uses and disclosures of substance, use and disorder ("SUD") records), the description of such use or disclosure must reflect the more stringent law,

- for each use and disclosure for TPO or uses and disclosures without an authorization, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required and other applicable law, such as 42 CFR Part 2,

- contain a description of the types of uses and disclosures that require an authorization and that an authorization may be revoked,

- a statement adequate to put the individual on notice of the potential for information disclosed by the plan, may be subject to redisclosure by the recipient and may no longer be protected,

- a statement that if SUD treatment records are received from a Part 2 Program, or testimony relaying the content of such records, the information will not be used or disclosed in civil, criminal, administrative, or legislative proceedings against the individual unless based on written consent, or a court order after notice and an opportunity to be heard is provided to the individual or the holder of the record, as provided by 42 CFR Part 2. A court order authorizing use or disclosure must be accompanied by a subpoena or other legal requirement compelling disclosure before the requested record is used or disclosed; or

- contain a statement of individual's rights with respect to PHI and a brief description of how the individual may exercise these rights, as follows:

    - The right to request restrictions on certain uses and disclosures of PHI, including a statement that the covered entity is not required to agree to a requested restriction;

    - The right to receive confidential communications of PHI;

    - The right to inspect and copy PHI;

    - The right to amend PHI,

    - The right to an accounting of disclosures of PHI; and

    - The right of an individual, including an individual who has agreed to receive notice electronically, to obtain a paper copy of the notice.

- note the Plan's duties as the Covered Entity, as follows:

- contain a statement that the Plan is required by law to maintain the privacy of PHI, to provide individuals with notice of its legal duties and privacy practices and notify affected individuals following a Breach of Unsecured PHI;

- a statement that the Plan is required to abide by the terms of the notice currently in effect; and

- a statement that the Plan reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains and how it will provide individuals with a revised notice.

- address how and where to complain,

- note the name, or title, and telephone number of a person or office to contact for further information and

- indicate the effective date of the Privacy Notice.

E. **Privacy Notice Revisions**: The Plan will promptly revise the Privacy Notice whenever there is a Material Revision to the uses and disclosures, the individual's rights, the Plan's legal duties, or other privacy practices stated in the Privacy Notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected

F. **Website and Electronic Privacy Notice obligations**: A Covered Entity (e.g. the Plan) that maintains a website that provides information about the Plan's customer service or benefits, must prominently post the Privacy Notice on that website and make the Privacy Notice available electronically through the website.

G. **E-mail Privacy Notice Distribution**: The Plan may provide the Privacy Notice to an individual by e-mail **IF** the individual requests that such notice be provided via email. If the Plan knows that the e-mail transmission failed, a paper copy of the Privacy Notice is to be provided. An individual who received an e-mail transmission of a Privacy Notice retains the right to obtain a paper copy from the Plan upon request.

H. **Documentation of Privacy Notice Distribution**: The Plan will document compliance with the HIPAA Rules' Privacy Notice obligations by retaining copies of the Privacy Notices the Plan issues.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Material Revisions** are changes to the uses and disclosures of PHI, an individual's rights, the duties of the Plan or other privacy practices stated in the Privacy Notice.

- **Named Insured** means the employee covered under the Plan.

PROCEDURES

1. **Privacy Notice Distribution**: The Plan will satisfy the requirements of the HIPAA Rules by providing the Privacy Notice to the Named Insured (covered employee) of the Plan; however, Name Insured will be encouraged to share the Privacy Notice with other family members covered under the Plan. The distribution of the Plan's Privacy Notice is handled by the Administrative Office in compliance with the following standards:

   a. **Initial Privacy Notice Distribution:** Before April 14, 2003, the Plan's initial Privacy Notice was sent by first class US mail to all Named Insureds who were covered under the Plan as of the date of the mailing.

   b. **New Enrollee Distribution:** The Administrative Office will distribute a Privacy Notice to newly covered individuals. The method of distribution will be by US mail. The Administrative Office on behalf of the Plan will retain proof of the Privacy Notice distribution.

   c. **Distribution of Revised Privacy Notice:** Whenever there is a Material Revision to the Privacy Notice, the revised Privacy Notice will be distributed as follows:

      - If a website exists for the Plan, the Plan will prominently display the Privacy Notice on its website by the effective date of the Material Revision to the Privacy Notice. Additionally, the Plan will provide the revised Privacy Notice or information about the Material Revision and how to obtain the revised Privacy Notice, in its next annual mailing to individuals then covered by the Plan; or

      - If the Plan does not maintain a website or the Privacy Notice is not posted on its website by the effective date of the Material Revision, the Plan will provide the revised Privacy Notice, or information about the Material Revision and how to obtain the revised Privacy Notice, to individuals then covered by the Plan within 60 days of the Material Revision to the Privacy Notice.

      The Administrative Office will retain a copy of the revised Privacy Notice along with a copy of the distribution list.

   d. **Upon Request:** The Administrative Office will distribute a Privacy Notice to a covered individual upon verbal or written request. The Administrative Office on behalf of the Plan will retain proof of Privacy Notice request and distribution dates.

   e. **Reminder Every Three Years:** No less than every three years, the Administrative Office will notify the Named Insureds that a Privacy Notice is available and how to obtain a copy of the Privacy Notice. This notification will be sent by regular mail.

   f. Note that if any of the Fund's health benefits are insured, a Named Insured should also receive a HIPAA Privacy Notice from each insurance company/HMO vendor. Neither the Plan nor its Privacy & Security Officer is responsible for Privacy Notice distribution by other covered entities.

2. **Privacy Notice Content:** The Privacy & Security Officer will ensure that the content of the Plan's Privacy Notices contain the required elements, as outlined in in Section 164.520(b) of the HIPAA Privacy Rule.

3. **Privacy Notice Revisions:**

   a. All requests for revision of the Privacy Notice are to be reviewed by the Privacy & Security Officer.

   b. The Privacy & Security Officer and Fund Counsel will review the Privacy Notice on a periodic basis and make any necessary changes to the Privacy Notice, assuring that such changes remain in compliance with the required content obligations of the Privacy Notice.

4. Website Privacy Notice Procedures: This Plan maintains a website that provides information about the Plan's customer service or benefits; therefore, this Plan must prominently post the Privacy Notice on that website and allow the printing of the Privacy Notice from the website.

   The Privacy & Security Officer or their designee will provide the company that maintains the website, a revised Privacy Notice at the time of any Material Revisions and request that any prior version of the Privacy Notice be removed from the website and the new Privacy Notice be posted on the website as of the effective date of the Material Revision.

   The Privacy & Security Officer or their designee will ensure that the new Privacy Notice is prominently posted and available on the website.

5. **E-mail Privacy Notice Procedures:** The Plan does not allow e-mail transmission of the Privacy Notice. The only time that a Privacy Notice may be emailed is if a Participant calls and requests a copy of the Privacy Notice be emailed to him or her.

6. **Documentation of Privacy Notice Distribution**: The Privacy & Security Officer will maintain a copy of all versions and revisions of the Privacy Notice. The Administrative Office will retain a copy of the distribution list in accordance with the Plan's Record Retention Policy.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Sections 164.502(a)(5)(iii) and 164.520
- 42 CFR Part 2
- The Plan's Privacy & Security Officer.
- Plan's Record Retention Policy

POLICY STATEMENT.

This policy and procedure is adopted pursuant to Section 164.530(a) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). If the privacy rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

At all times, the Plan will have a delineation of roles and responsibilities, as needed, to fulfill the requirements of the HIPAA and HITECH Rules, state privacy laws, and the terms of Business Associate Agreements. As part of such delineation, the Plan has designated a Privacy & Security Officer and a HIPAA Oversight Committee, warranted to meet regulatory and operational requirements.

PROCEDURES

1. **Roles and Responsibilities.**

   a. Privacy & Security Officer. The Plan has designated a Privacy & Security Officer who is responsible for overseeing the Plan's HIPAA compliance efforts, including:

   - Establishing a HIPAA Oversight Committee and serving in a leadership role on same Committee;
   - Developing and implementing the Plan's privacy, security and breach notification policies and procedures and core document templates (such as authorization and notice of privacy practices);
   - Directing or arranging for initial and periodic risk assessments, as necessary, of compliance with the Plan's security policies and procedures, including a thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the Fund;
   - Participating in the identification of Business Associates/trading partners and in the ongoing compliance monitoring and inventory of Business Associate Agreements/trading partner agreements;
   - Ensuring Business Associate Agreements and trading partner agreements are secured with all Plan Business Associates and trading partners; any deviations from the template agreements will be negotiated and agreed to by the Fund's Legal Counsel.
   - Developing, or confirming the development of, initial and ongoing privacy and security training for the Fund's workforce members (including initial training for new workforce members and periodic update training for current workforce members);
   - Maintaining current knowledge of applicable federal and state privacy and security laws and regulations and confirming, in consultation with Fund

Legal Counsel, that necessary revisions are made to the Plan's privacy, security and breach notification policies and procedures, core document templates, and plan documents for updating purposes;

- Performing initial and periodic assessments of compliance with the Plan's privacy, security and breach notification policies and procedures, reporting any known or potential problems to the Fund and to the Fund's Legal Counsel, as appropriate, and addressing same problems;

- Responding to individual participants' privacy and security-related concerns and/or complaints with respect to the Plan's privacy and security policies and procedures;

- Development and implementation of a privacy and security incident response plan, including maintaining a log of all complaints/reported incidents, related investigations, and any follow-up activities related to the Plan and/or its Business Associates, and confirming prevention, detection, containment, and correction of security incidents;

- Addressing requests relating to individual rights to inspect, amend and/or restrict access to protected health information;

- Reviewing and following up on, as appropriate, requests for disclosure of PHI, whether by individuals or third parties;

- Identifying and tracking of disclosures of participant information and accounting for such disclosures as required by HIPAA;

- Assisting the Trustees or other designated individuals in developing appropriate disciplinary measures when workforce members violate the Plan's privacy, security and/or breach notification policies and procedures;

- Developing appropriate administrative, physical and technical safeguards for the protection of the Plan's PHI;

- Cooperating with HHS's Office of Civil Rights, state agencies and other regulatory authorities, in coordination with the Fund's Legal Counsel in responding to any compliance reviews, audits or investigations; and

- Implementing corrective measures to address any identified gaps or findings stemming from the reviews, audits or investigations noted above.

b. **HIPAA Oversight Committee.** Will be responsible for guiding implementation of strategic initiatives and promoting the privacy and security of health information and management system, including:

- Review and make any recommendations to the Board of Trustees concerning new or updated Privacy and/or Security policies and procedures;

- Review reports provided by the Privacy & Security Officer (e.g. incident, violation, complaint, risk assessment, risk management) - guide and support any remediation efforts;

- Review vendor list on an ongoing basis pursuant to which the Privacy & Security Officer ensures that the list is maintained current and BAAs are in place as necessary;

- Review vendor audit reports and guide and support any remediation efforts;

- Review any new or changes to the Fund's information systems, devices, equipment, etc. that would access, disclose or maintain electronic PHI;

- Notify the Privacy & Security Officer when new Trustees are appointed to ensure HIPAA training is completed timely;

- Review other HIPAA related reports (e.g. status of Trustee HIPAA training) provided by the Privacy & Security Officer;

- Report to the Privacy & Security Officer any known violation of the Privacy or Security Policies and Procedures, and assist in any consequent investigation, sanction, and/or mitigation;

- Review status reports concerning HHS' Office of Civil Rights, state agencies and other regulatory authorities' audits, if applicable, presented by the Privacy & Security Officer.

These lists provide an overview of the responsibilities of the respective individuals and are not meant to serve as all-inclusive descriptions.

The Committee shall meet at least annually and otherwise as necessary.

2. **DESIGNATIONS AND CONTACT INFORMATION.**

The Plan has designated the following individual to serve as the Privacy & Security Officer:

Cory Crandell
8441 Gulf Freeway, Suite 304
Houston, TX 77017
Email: ccrandell@benefitresourcesinc.com

HIPAA Oversight Committee:
Plan Privacy & Security Officer
Board of Trustees

MAINTENANCE.

This Policy will be reviewed by the Privacy & Security Officer every year or as deemed appropriate based on changes in business operations, federal or state law, or regulatory

requirements. Recommendations for any changes shall be made to the Privacy & Security Officer and approved as set forth above.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES.

- 45 C.F.R 164.530(a)
- The Plan's Privacy & Security Officer
- Fund's Legal Counsel
- Fund's Consultant

HIPAA POLICY AND PROCEDURE - THE PRIVACY & SECURITY OFFICER

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(a) and 164.308(a)(2) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

- The Plan has designated a privacy and security official who is responsible for the development and implementation of the HIPAA policies and procedures of the Plan. The Plan must document the personnel designation.

- The Plan has designated a contact person or office who is responsible for receiving complaints about the Privacy policies and procedures of this Plan and who is able to provide further information about matters covered by the required HIPAA Privacy Notice. The Plan must document the personnel designation.

PROCEDURES

1. Under this Plan, the title of the "Privacy & Security Officer" is the person who will receive complaints about the Privacy policies and procedures of the Plan as noted above.

2. Questions regarding the HIPAA Privacy Notice will be answered by the Privacy & Security Officer or their designee.

3. The Privacy & Security Officer will follow the job description associated with this position and will oversee the Plan's HIPAA compliance operations, policies and procedures.

4. The Privacy & Security Officer and their designees will undergo a background check to help ensure that these individuals are appropriate to access PHI. The Fund Office will coordinate this process. The Fund Office shall provide any information of concern to the Fund's legal counsel for review.

5. The Privacy & Security Officer will use the resources listed below in order to answer questions and implement the Policies and Procedures.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR Section 164.530(a)
- The Plan's Privacy & Security Officer

POLICY STATEMENT

This policy and procedure is adopted pursuant to Sections 164.508 of the HIPAA Rules and 42 CFR Part 2. If these Rules are changed by the Department of Health and Human Services (HHS), the Plan will follow the revised rules.

SECTION 164.508 - AUTHORIZATION - USES AND DISCLOSURES

A. Authorizations for uses and disclosures —

1) ***Authorization required: General rule.*** Except as otherwise permitted or required by the HIPAA Rules, a covered entity may not use or disclose PHI without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure must be consistent with such authorization.

2) ***Authorization required: Psychotherapy notes.*** Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

   a) To carry out the following treatment, payment, or health care operations:

      i) Use by the originator of the psychotherapy notes for treatment;

      ii) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

      iii) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

   b) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

3) ***Authorization required: Marketing.***

   a) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

      i) A face-to-face communication made by a covered entity to an individual; or

      ii) A promotional gift of nominal value provided by the covered entity.

   b) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

4) ***Authorization required: Sale of protected health information.***

a) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart.

b) Such authorization must state that the disclosure will result in remuneration to the covered entity.

B. General requirements —

1) ***Valid authorizations.***

a) A valid authorization is a document that meets the requirements in paragraph A.3)b), A4)b) of this section and paragraph C. "Core Elements and Requirements" of this section.

b) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

2) ***Defective authorizations.*** 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 by the covered entity to have occurred;

b) The authorization has not been filled out completely;

c) The authorization is known by the covered entity to have been revoked;

d) The authorization violates paragraph B.3) or B.4) of this section, if applicable;

e) Any material information in the authorization is known by the covered entity to be false.

3) ***Compound authorizations.*** An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:

a) An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph B.4)(a) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

b) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

c) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph B.4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph B.4) of this section does not apply to a compound authorization created in accordance with paragraph B.3)a) of this section.

4) ***Prohibition on conditioning of authorizations.*** A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

a) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

b) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

i) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

ii) The authorization is not for a use or disclosure of psychotherapy notes under paragraph A.2) of this section; and

c) A covered entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.

5) ***Revocation of authorizations.*** An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

a) The covered entity has taken action in reliance thereon; or

b) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

6) ***Documentation.*** A covered entity must document and retain any signed authorization for a minimum of six years from the date of its creation or the date when it was last in effect, whichever is later.

C. Core elements and requirements —

1) ***Core elements.*** A valid authorization under this section must 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 persons, authorized to make the requested use or disclosure.

c) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

d) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

e) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

f) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

2) ***Required statements.*** In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

a) The individual's right to revoke the authorization in writing, and either:

i) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

ii) To the extent that the exceptions to the right to revoke the authorization are included in the Plan's Notice of Privacy Practices, a reference to such notice.

b) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

i) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph B.4) of this section applies; or

ii) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph B.4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

c) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

3) ***Plain language requirement.*** The authorization must be written in plain language.

4) ***Copy to the individual.*** If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

SECTION 42 CFR PART 2, Subpart C —
USES AND DISCLOSURES WITH PATIENT CONSENT

1) Section 2.31 Consent Requirements –

a) ***Required elements for written consent.*** A written consent to a use or disclosure under the regulations in this part may be paper or electronic and must include:

i) The name of the patient.

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

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

iv) ***General requirement for designating recipients.***

(1) The name(s) of the person(s), or class of persons, to which a disclosure is to be made ("recipient(s)"). For a single consent for all future uses and disclosures for treatment, payment, and health care operations, the recipient may be described as "my treating providers, health plans, third-party payers, and people helping to operate this program" or a similar statement.

(2) ***Special instructions for intermediaries.*** Notwithstanding paragraph 1)a)iv)(1) of this section, if the recipient entity is an intermediary, a written consent must include the name(s) of the intermediary(ies) and:

(a) The name(s) of the member participants of the intermediary; or

(b) A general designation of a participant(s) or class of participants, which must be limited to a participant(s) who has a treating provider relationship with the patient whose information is being used or disclosed.

(3) ***Special instructions when designating certain recipients.*** If the recipient is a covered entity or business associate to whom a record (or information contained in a record) is disclosed for purposes of treatment, payment, or health care operations, a written consent must include the statement that the patient's record (or information contained in the record) may be redisclosed in accordance with the permissions contained in the HIPAA regulations, except for uses and disclosures for civil, criminal, administrative, and legislative proceedings against the patient.

v) A description of each purpose of the requested use or disclosure.

(1) The statement "at the request of the patient" is a sufficient description of the purpose when a patient initiates the consent and does not, or elects not to, provide a statement of the purpose.

(2) The statement, "for treatment, payment, and health care operations" is a sufficient description of the purpose when a patient provides consent once for all such future uses or disclosures for those purposes.

(3) If a Part 2 program intends to use or disclose records to fundraise on its own behalf, a statement about the patient's right to elect not to receive any fundraising communications.

vi) The patient's right to revoke the consent in writing, except to the extent that the Part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it, and how the patient may revoke consent.

vii) An expiration date or an expiration event that relates to the individual patient or the purpose of the use or disclosure. The statement "end of the treatment," "none," or similar language is sufficient if the consent is for a use or disclosure for treatment, payment, or health care operations. The statement "end of the research study" or similar language is sufficient if the consent is for a use or disclosure for research, including for the creation and maintenance of a research database or research repository.

viii) The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who has been adjudicated as lacking the capacity to make their own health care decisions or is deceased, the signature of a person authorized to sign under § 2.15. Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.

ix) The date on which the consent is signed.

x) A patient's written consent to use or disclose records for treatment, payment, or health care operations must include all of the following statements:

(1) The potential for the records used or disclosed pursuant to the consent to be subject to redisclosure by the recipient and no longer protected by this part.

(2) The consequences to the patient of a refusal to sign the consent.

b) ***Consent required: SUD counseling notes.***

i) Notwithstanding any provision of this section, a Part 2 program must obtain consent for any use or disclosure of SUD counseling notes, except:

(1) To carry out the following treatment, payment, or health care operations:

(a) Use by the originator of the SUD counseling notes for treatment;

(b) Use or disclosure by the part 2 program for its own training programs in which students, trainees, or practitioners in SUD treatment or mental health learn under supervision to practice or improve their skills in group, joint, family, or individual SUD counseling; or

(c) Use or disclosure by the part 2 program to defend itself in a legal action or other proceeding brought by the patient;

(2) A use or disclosure that is required by § 2.2(b) or permitted by § 2.15(b); § 2.53 with respect to the oversight of the originator of the SUD counseling notes; § 2.63(a); § 2.64.

ii) A written consent for a use or disclosure of SUD counseling notes may only be combined with another written consent for a use or disclosure of SUD counseling notes.

iii) A part 2 program may not condition the provision to a patient of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of a written consent for a use or disclosure of SUD counseling notes.

c) ***Expired, deficient, or false consent.*** A disclosure may not be made on the basis of a consent which:

i) Has expired;

ii) On its face substantially fails to conform to any of the requirements set forth in paragraph (a) of this section;

iii) Is known to have been revoked; or

iv) Is known, or through reasonable diligence could be known, by the person holding the records to be materially false.

d) ***Consent for use and disclosure of records in civil, criminal, administrative, or legislative proceedings.*** Patient consent for use and disclosure of records (or testimony relaying information contained in a record) in a civil, criminal, administrative, or legislative investigation or proceeding cannot be combined with a consent to use and disclose a record for any other purpose.

2) SECTION 2.32 - Notice and copy of consent to accompany disclosure

a) Each disclosure made with the patient's written consent must be accompanied by one of the following written statements:

i) ***Statement 1.***

This record which has been disclosed to you is protected by Federal confidentiality rules (42 CFR part 2). These rules prohibit you from using or disclosing this record, or testimony that describes the information contained in this record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against the patient, unless authorized by the consent of the patient, except

as provided at 42 CFR 2.12(c)(5) or as authorized by a court in accordance with 42 CFR 2.64 or 2.65. In addition, the Federal rules prohibit you from making any other use or disclosure of this record unless at least one of the following applies:

(1) Further use or disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2.

(2) You are a covered entity or business associate and have received the record for treatment, payment, or health care operations, or

(3) You have received the record from a covered entity or business associate as permitted by 45 CFR part 164, subparts A and E.

A general authorization for the release of medical or other information is NOT sufficient to meet the required elements of written consent to further use or redisclose the record (see 42 CFR 2.31).

ii) ***Statement 2.*** "42 CFR part 2 prohibits unauthorized use or disclosure of these records."

b) Each disclosure made with the patient's written consent must be accompanied by a copy of the consent or a clear explanation of the scope of the consent provided.

3) Section 2.33 Uses and disclosures permitted with written consent.

a) If a patient consents to a use or disclosure of their records consistent with § 2.31, the following uses and disclosures are permitted, as applicable:

i) A Part 2 program may use and disclose those records in accordance with that consent to any person or category of persons identified or generally designated in the consent, except that disclosures to central registries and in connection with criminal justice referrals must meet the requirements of §§ 2.34 and 2.35, respectively.

ii) When the consent provided is a single consent for all future uses and disclosures for treatment, payment, and health care operations, a Part 2 program, covered entity, or business associate may use and disclose those records for treatment, payment, and health care operations as permitted by the HIPAA regulations, until such time as the patient revokes such consent in writing.

b) If a patient consents to a use or disclosure of their records consistent with § 2.31, the recipient may further disclose such records pursuant to a court order authorizing the use and disclosure and as follows:

i) When disclosed for treatment, payment, and health care operations activities to a covered entity or business associate, such recipient may further disclose those records in accordance with the HIPAA regulations, except for uses and disclosures for civil, criminal, administrative, and legislative proceedings against the patient.

ii) When disclosed with consent given once for all future treatment, payment, and health care operations activities to a Part 2 program that is not a covered entity or business associate, the recipient may further disclose those records consistent with the consent.

iii) When disclosed for payment or health care operations activities to a lawful holder that is not a covered entity or business associate, the recipient may further disclose those records as may be necessary for its contractors, subcontractors, or legal representatives to carry out the payment or health care operations specified in the consent on behalf of such lawful holders.

c) Lawful holders, other than covered entities and business associates, who wish to redisclose patient identifying information pursuant to paragraph b)iii) of this section must have in place a written contract or comparable legal instrument with the contractor or voluntary legal representative, which provides that the contractor, subcontractor, or voluntary legal representative is fully bound by the provisions of this part upon receipt of the patient identifying information. In making any such redisclosures, the lawful holder must furnish such recipients with the notice required under § 2.32; require such recipients to implement appropriate safeguards to prevent unauthorized uses and disclosures; and require such recipients to report any unauthorized uses, disclosures, or breaches of patient identifying information to the lawful holder. The lawful holder may only redisclose information to the contractor or subcontractor or voluntary legal representative that is necessary for the contractor, subcontractor, or voluntary legal representative to perform its duties under the contract or comparable legal instrument. Contracts may not permit a contractor, subcontractor, or voluntary legal representative to redisclose information to a third party unless that third party is a contract agent of the contractor or subcontractor, helping them provide services described in the contract, and only as long as the agent only further discloses the information back to the contractor or lawful holder from which the information originated.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing HIPAA Authorizations and Consents to contracted Business Associates consistent with Sections 164.508 of the HIPAA Rules and 42 CFR Part 2. The contracted Business Associates are responsible for implementing procedures for processing HIPAA Authorizations and Consents. Such procedures will be provided to the Plan upon request. The Business Associates will retain signed authorizations and consents consistent with the Plan's Record Retention Policy.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions

ADDITIONAL RESOURCES

- 45 CFR, Sections 164.508.

- 42 CFR Part 2
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502 (g) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

The Plan, through its contracted Business Associates will provide relevant PHI to personal representatives of an individual, unless, it is otherwise prevented by law from doing so.

1) **Individuals**: The Plan generally will treat a personal representative as the "individual" for purposes of the HIPAA Rules. Therefore the Plan generally will provide PHI about an individual only to and about that individual unless the law permits otherwise (such as the release of PHI for treatment payment and health care operation or with a signed authorization form or where an individual has formally elected a personal representative).

2) **Employee and Spouse:** Under this Plan, this Plan will NOT automatically honor an employee's spouse as the employee's personal representative and vice versa.

   Per Section 164.510(b)(3) of the regulation, the Plan may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes. This rule extends to the PHI of a deceased individual unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the Plan.

3) **Adults and Emancipated Minors:** If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, the Plan generally will treat such person as a personal representative with respect to PHI. Note that a power of attorney that does not include decisions related to health care in its scope would not be sufficient to create personal representative status for purposes of the HIPAA Rules. Thus, a person with an individual's power of attorney may or may not be the individual's personal representative for HIPAA privacy purposes, depending on whether the power of attorney includes authority to act on behalf of the individual in decisions related to health care.

4) **Unemancipated Minors**:

   a) If under applicable law a parent, guardian or other person acting "in loco parentis" (in place of the parent) has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, the Plan generally will treat such person as a personal representative with respect to PHI. However, such person may not be a personal representative of an unemancipated minor and the minor has the authority to act as an individual, with respect to PHI pertaining to a health care service if:

      i) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

ii) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

iii) A parent, guardian, or other person acting *in loco parentis* assents (agrees) to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

b) Notwithstanding the provisions of the above text regarding unemancipated minors:

i) As permitted by law, the Plan may disclose (or not disclose) PHI or provide access (or no access) to PHI about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis* in accordance with the Plan's policy and procedure on "Access to PHI."

ii) Where the parent, guardian, or other person acting *in loco parentis*, is **not** the personal representative (as described above in this policy) and as permitted by law the Plan may provide or deny access to a parent, guardian, or other person acting *in loco parentis*, (in accordance with the Plan's policy on "Access" to PHI) provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

5) **Deceased individuals:** If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the Plan generally will treat such person as a personal representative with respect to PHI relevant to such personal representation. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a deceased individual for a period of 50 years following the date of death. After 50 years has passed, the individually identifiable health information of the deceased individual is no longer considered to be PHI that is protected by the HIPAA Rules.

6) **Abuse, neglect, endangerment situations:** As permitted by law, the Plan may elect **not** to treat a person as the personal representative of an individual, provided that the conditions below are met:

a) The Plan has a reasonable belief that:

i) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

ii) Treating such person as the personal representative could endanger the individual.

b) The Plan, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

Emancipated Minor: Generally emancipated minors are under eighteen, not married, not serving in the armed forces, self-supporting for two years, not living with parents and have completely severed the

parental relationship as to all legal rights and liabilities, including care, custody, control and service for two years.

The Privacy & Security Officer (or their designee) should consult legal advice in situations where a minor wants to act as their own personal representative.

Emancipation is not available in every state in the United States. Where it is available, emancipation is a legal process by which minors can attain legal adulthood before reaching the age at which they would normally be considered adults (this is called the "age of majority"). The rights granted to legally emancipated minors might include the ability to sign legally binding contracts, own property, and keep one's own earning. However, each state has different laws governing emancipation and some states simply have no law or legal process concerning emancipation. In states where minors wish to become legally emancipated they will have to break new legal ground. Married minors are typically considered to be emancipated minors. **Family Member** means, with respect to an individual:

1. A dependent (as such term is defined in 45 CFR 144.103, which says " any individual who is or may become eligible for coverage under the terms of a group health plan because of a relationship to a participant"), of the individual; or

2. Any other person who is a first-degree, second-degree, third degree, or fourth degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

    a. First-degree relatives include parents, spouses, siblings, and children.

    b. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

    c. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

    d. Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Personal Representative is not specifically defined by the HIPAA Rules. For this Plan, it means any adult who has the authority by law or by written agreement from the individual, to act in place of that individual.

Individual means the person who is the subject of PHI.

PROCEDURES

The Plan Sponsor, on behalf of the Plan has delegated the responsibility for implementing this policy and procedures to contracted Business Associates. Those Business Associates are required to implement procedures in compliance with Section 164.502(g) of the HIPAA Rules on behalf of the Plan and shall implement procedures for recognizing personal representatives. Such procedures will be provided to the Plan upon request. The Business Associates will maintain personal representative designation and

revocation forms in compliance with the HIPAA Rules and the Plan's policy and procedure on Record Retention and Destruction.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.502 (g).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention and Destruction policy and procedure
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(b) and 514 (d) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

A. When using or disclosing PHI, or when requesting PHI from another Covered Entity or Business Associate, the Plan or Business Associate will make reasonable efforts to limit PHI to the **minimum necessary to accomplish the intended purpose of the use**, **disclosure or request**.

B. The Plan has implemented these policies and procedures for routine uses and disclosures. **This minimum necessary policy applies to oral, electronic, and written PHI.**

Minimum necessary standard does not apply to uses and disclosures:

- to or requests by a health care provider for treatment
- to the individual
- made in accordance with a valid authorization
- made to the Secretary of the Dept. of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated.
- for which an authorization or opportunity to agree or disagree is not required under the regulation.
- that are required for compliance with the general rules under §164.502.
- Required for compliance with HIPAA electronic data interchange (EDI) transaction standards.

C. In order to comply with the **minimum necessary requirements** the Plan will:

1. Identify those persons or classes of persons, as appropriate, in the **workforce who need access** to PHI to carry out their duties;
    - Identify the categories of PHI to which access is needed and the conditions appropriate to such access.
    - Make reasonable efforts to limit the access of its workforce as described above.
2. Disclose PHI, as follows:
    - For routine disclosures made on a recurring basis, the Plan will establish procedures that limit PHI to the amount reasonably necessary to achieve the purpose of the disclosure;

- For other disclosures the Plan will develop and use criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose of the disclosure; and

- Review non-routine requests for disclosure on an individual basis.

- To the extent practicable, the Plan will only use, disclose or request limited data set information. This limited data set information excludes the following direct identifiers of the individual or their relatives, employers or household members:

  1) Names

  2) Postal address information except town, city, state and zip code

  3) Telephone and fax numbers

  4) Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers or certificate/license numbers

  5) Vehicle identifiers and serial numbers including license plate numbers, and device identifiers and serial numbers

  6) Email addresses, web universal resource locators (URLs), and internet protocol (IP) address numbers and

  7) Biometric identifiers such as finger and voiceprints, full face photographic images and any comparable images.

  Limited data set information may include dates related to the individual such as birth date or dates of admission or discharge, and certain geographic information such as an individual's town, city, state or zip code.

3. Rely upon a requested disclosure as being the minimum necessary for the stated purpose, when the information is requested by one of the following and the requestor represents that the information is the minimum necessary for the stated purpose.

   - public officials that are permitted under 164.512 (see this Plan's policy on "Disclosure of PHI for Public Health, etc.");

   - another Covered Entity;

   - a professional who is a member of the Plan's workforce or is a **Business Associate** of the Plan for the purpose of providing professional services to the Plan;

   - documentation or representations that comply with the applicable requirements related to research.

4. Request information from another Covered Entity that is:

   - Limited to that which is reasonably necessary to accomplish the purpose of the request;

- For routine, recurring basis, in accordance with the Plan's standard procedures;

- For other requests, in accordance with specific criteria. Such requests will be reviewed on an individual basis.

5. The Plan will not request an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the use, disclosure, or request.

D. **Disclosures to Business Associates.**

1. A Covered Entity may disclose PHI to a Business Associate and may allow a Business Associate to create, receive, maintain, or transmit PHI on its behalf, if the Covered Entity obtains satisfactory assurance that the Business Associate will appropriately safeguard the information. A Covered Entity is not required to obtain such satisfactory assurances from a Business Associate that is a subcontractor.

2. A Business Associate may disclose PHI to a Business Associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, if the Business Associate obtains satisfactory assurances, in accordance with your Business Associate Agreement, that the subcontractor will appropriately safeguard the information.

The satisfactory assurances required by disclosures to Business Associates must be documented through a written contract or other written agreement or arrangement with the Business Associate that meets the applicable requirements of your Business Associate Agreement.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Workforce** means Trustees, Fund employees, volunteers, trainees, and other persons whose conduct in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.

PROCEDURES

The Trustees are the Plan's sponsor and all Trustees and alternate trustees thereof are designated as persons entitled to receive PHI. In general, potential PHI will be de-identified before being transmitted to Trustees or alternate trustees. If de-identification is not practical, the Trustees will request only minimum necessary information. The Trustees will use PHI only for Plan administration activities and not for employment or union-related actions or for any purpose unrelated to Plan administration.

Business Associates are required to implement procedures for limiting PHI to the minimum necessary in compliance with Section 164.502 (b) and 514 (d) of the HIPAA Rules. Copies of such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.502.
- The Plan's Privacy & Security Officer.

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514 (h) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

General Policy:

The Plan **must verify the identity of an individual or entity requesting PHI ,** and verify the authority of such individual to have access to PHI, before the PHI is disclosed to the individual, **if** the identity or any such authority of the individual is not known to the Plan.

The Plan will obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement or representation is a condition of disclosure of PHI under HIPAA. The Plan may rely, if such reliance is reasonable under the circumstances, on documentation, statements or representations that, on their face, meet HIPAA's requirements.

Identity of Public Officials:

The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

1. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

2. If the request is in writing, the request is on the appropriate government letterhead; or

3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

The Plan may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

- If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

The verification requirements of this paragraph are met if the Plan relies on the exercise of professional judgment in making a use or disclosure.

Emergency Situation: Imminent Serious Threat to Health and Safety:

A disclosure to an individual or entity in accordance with Section 164.512(j)(1)(i) (other than to a public official) to avert an imminent threat to health or safety is allowed without further verification if the Plan has a good faith belief that the disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, and the disclosure is to a person reasonably able to prevent or lessen the threat.

- If these conditions are met no further verification is needed.
- In such emergencies the Plan is not required to demand written proof that the person requesting the PHI is legally authorized.
- The Plan can reasonably rely on verbal representations.
- The Plan will document such disclosure.

Where Verification is Not Required:

This policy does not apply and verification is not required for disclosures made under Section 164.510(a) regarding disclosures **for facility directories**, and 164.510(b) disclosures **for involvement in an individual's care and for notification purposes**.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates are required to implement procedures for verification of identity, in compliance with Section 164.514 (h) of the HIPAA Rules. Copies of such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.514(h).
- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE FOR PHYSICAL, ADMINISTRATIVE AND TECHNICAL SAFEGUARDS FOR PHI

POLICY STATEMENT

This Policy and Procedure is adopted pursuant to Section 164.530(c) and 164.308, 164.310 and 164.312 of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan has no employees and, while the Plan Sponsor is entitled to receive PHI, in general, the information is required to be de-identified before it is sent to the Plan Sponsor. If de-identification is not practical, minimum necessary information is sent in **non-electronic** media such as fax, mail, messenger or phone.

The Plan's functions, including creation and maintenance of its records, are carried out by the Business Associates of the Plan. Neither the Plan nor the Plan Sponsor own or control any of the equipment or media used to create, maintain, receive, and transmit PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Business Associates. Accordingly, the Business Associates create, receive, maintain, and transmit all PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit PHI relating to the Plan, and control their employees, agents, and subcontractors who have access to PHI relating to the Plan. The Plan will request appropriate changes from the Business Associate if they become aware of any potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI relating to the Plan. That ability lies solely with the Plan's Business Associates.

The Plan will establish appropriate procedures to safeguard PHI physically, administratively and technically. The Plan will take reasonable steps to limit incidental use or disclosure of PHI by anyone other than those individuals specifically authorized to work with PHI as part of Plan operations.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Trustees are the Plan's sponsor and all Trustees and alternate trustees (collectively "Trustee") thereof are designated as persons entitled to receive PHI. The Trustees will adhere to the following procedures for safeguarding PHI:

1) **Requesting PHI** – In general, Trustees request and receive de-identified PHI. PHI is only requested for Plan administration purposes. When de-identification is not feasible, the Trustees will request/receive minimum necessary information in non-electronic format.

2) **Storing PHI** – In general, PHI is not maintained by Trustees. PHI received by Trustees is properly destroyed (e.g. shredded) or returned to the Business Associate for proper storage/destruction.

3) **Transmitting PHI** – In general, the Trustees do not transmit PHI. However, should the Trustees be required to transmit PHI for Plan administration purposes, they will do so in non-electronic format and in compliance with HIPAA.

If there are no set guidelines in place, PHI may be transmitted by Trustees as follows:

a) Paper PHI will be transmitted as follows:

(1) in person to the individual or Business Associate that requested the PHI

(2) first-class mail to the last known address of the individual

(3) other secure transmission methods as agreed upon by Trustee and receiver

The Trustees will not include PHI in outgoing e-mail messages or in attachments to e-mails. The Plan Sponsor, on behalf of the Plan has the right to monitor both internal and external e-mails (incoming and outgoing) to ensure the security of PHI.

The Privacy & Security Officer may perform periodic audits of the e-mails sent to Trustees to ensure that the e-mails are void of PHI.

Business Associates are required to implement procedures, in compliance with Section 164.530(c) of the Final Rules and 164.308, 164.310 and 164.312 of the Security Rules, on behalf of the Plan and shall implement procedures for safeguarding physical, administrative and technical PHI. Compliance with such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions and Breach in this manual.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.530(c), 164.308, 164.310 and 164.312.
- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE FOR CERTIFICATION AND PLAN DOCUMENT AMENDMENT

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.504(f) and 164.314(b) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

Plan Documents will be amended (in compliance with 164.504(f) and 164.314(b) requirements for group health plans) to:

a. Establish permitted and required uses and disclosures of PHI by the Plan Sponsor;

b. Provide that the Group Health Plan will disclose PHI to the Plan Sponsor only upon receipt of a certification by the Plan Sponsor that the plan documents have been amended to incorporate permitted and required uses and disclosures of PHI by the Plan Sponsor.

Plan Sponsor Certification - The Plan Sponsor will provide written certification that Group Health Plan Documents have been amended to incorporate the requirements of the HIPAA Rules at Sections 164.504 (f) and 164.314(b) and that the Plan Sponsor agrees to comply with the HIPAA Rules. This written certification will allow a health insurance issuer (hereafter called health insurance company), HMO, or the Group Health Plan (the Plan) to disclose individually identifiable health information to the Plan Sponsor for Plan Administration functions only.

The Plan can disclose PHI to the Board of Trustees if the Board of Trustees voluntarily agrees to use and disclose the information only as permitted or required by the regulation. PHI may be used only for plan administration functions (e.g. claim appeals) performed on behalf of the Group Health Plan which are specified in plan documents.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Health Insurance Issuer** means (per Section 2791(b)(2) of the Public Health Service Act) an insurance company, insurance service, or insurance organization (including an HMO) which is licensed to engage in the business of insurance in a State and which is subject to State law which regulates insurance (within the meaning of Section 514(b)(2) of ERISA. Such term does not include a group health plan.

- **Plan Sponsor** means the Board of Trustees of Pipe Fitters Local Union No. 211 Welfare Trust Fund.

- **Plan administration functions** means administration functions (such as claim appeals) performed by the Plan sponsor of a Group Health Plan on behalf of the Group Health Plan and excludes functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor. It does not include any employment or union-related functions or functions in connection with any other benefits or benefit plans not regulated by HIPAA Privacy.

PROCEDURES

1. The Plan Sponsor, on behalf of the Plan, has amended applicable Plan Document(s) to be consistent with the use and disclosure of PHI permitted in the regulations.

2. The original or a copy of the original Certification Statement will be retained by the Privacy & Security Officer in accordance with the Plan's policy and procedure on record retention.

3. Copies of the original certification statement may be provided by the Privacy & Security Officer to interested parties as needed to prove that the Plan Sponsor voluntarily agrees to use and disclose the PHI only as permitted or required by the regulation.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.504 (f) and 164.314(b).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 160.103, 164.502(e), 164.504, 164.532, 164.314(a)(1) and 164.314 (a)(2)(iii) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

A The Plan permits the Business Associates to create, receive, maintain, or transmit PHI, including electronic PHI, on its behalf. The Plan has obtained or will obtain satisfactory assurances from all Business Associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA Rules. The Plan will coordinate a Business Associate Agreement or other arrangement as required by the HIPAA Rules.

B The contract between the Plan and a Business Associate will:

1. Establish the permitted and required uses and disclosures of PHI by the Business Associate. The contract will not authorize the Business Associate to use or further disclose the information in a manner that would violate the requirements of the regulations, except that:

    a. The contract may permit the Business Associate to use and disclose PHI for the proper management and administration of the Business Associate; and

    b. The contract may permit the Business Associate to provide data aggregation services relating to the health care operations of the Plan.

2. At a minimum, provide that the Business Associate will:

    a. Not use or further disclose the information other than as permitted or required by the contract or as required by law;

    b. Implement administrative, physical and technical safeguards to prevent use or disclosure of the information, including electronic PHI, other than as provided for by its contract;

    c. Implement administrative, physical and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that the Business Associate creates, receives, maintains or transmits on behalf of the Plan;

    d. Report to the Plan any use or disclosure of the information not provided for by its contract of which it becomes aware including security incidents or breaches of unsecured PHI;

    e. Take any contractually required steps with respect to breach notification requirements;

f. Ensure that any agents to whom it provides PHI received from, or created or received by the Business Associate on behalf of, the Plan agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information;

g. Make available PHI in accordance with § 164.524 (regarding access of individuals to PHI);

h. Make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526 (regarding amendment of PHI);

i. Make available the information required to provide an accounting of disclosures in accordance with § 164.528 (regarding accounting of disclosure of PHI);

j. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the Plan available to the Secretary for purposes of determining the Plan's compliance with this subpart; and

k. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the Plan that the Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

3. **Violation of Privacy or Security by Business Associate:** If the Plan knows of a pattern of activity or practice of a Business Associate or a subcontractor of the Business Associate that constitutes a material breach or violation of the Business Associate's or subcontractor's obligation under the contract or other arrangement, the Plan will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Plan reserves the right to terminate the contract or arrangement, or if termination is not feasible, report the problem to the Secretary for the Department of Health and Human Services.

4. The contract or other arrangement between the Plan and Business Associate may permit the Business Associate to use the PHI received by the Business Associate in its capacity as a Business Associate to the Plan, if necessary for the proper management and administration of the Business Associate; or to carry out the legal responsibilities of the Business Associate.

5. The contract or other arrangement between the Plan and the Business Associate may permit the Business Associate to disclose the PHI received by the Business Associate in its capacity as a Business Associate for disclosures required by law; or:

   a. The Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

b. The person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. The requirements of a Business Associate Agreement apply to the contract or other arrangement between a Business Associate and a Business Associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a Covered Entity and Business Associate.

6. The Plan will ensure that a Business Associate Agreement is signed with each Business Associate of the Plan as required.

7. The Plan will, in some instances, implement an extension of time for executing Business Associate Agreements. Extensions must be approved by the Privacy & Security Officer according to the following parameters:

   a. If there is any change in the signed contract between the Plan and a Business Associate, including a fee change, then a Business Associate Agreement will be executed at the same time the existing contract is modified.

   b. Regardless of whether a Business Associate Agreement has been obtained, the Plan will comply with the individual rights provisions of HIPAA (as applicable) and will permit the Secretary of Health and Human Services to inspect records.

8. The Plan will ensure that a Business Associate Agreement is obtained for all new Business Associate relationships .

The Plan will ensure that Business Associate Agreements are updated in compliance with the above step.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

A **Business Associate (BA)** means, with respect to a Covered Entity (the Plan), a person who:

1. On behalf of such Covered Entity or of an organized health care arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits PHI, in electronic and non-electronic format, for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20 (*outlined under Patient Safety Activities below*), billing, benefit management, practice management, and repricing; or

2. Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 *which is defined below*), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

3. A Covered Entity may be a Business Associate of another Covered Entity.

Business Associate includes:

a. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI.

b. A person that offers a personal health record to one or more individuals on behalf of a Covered Entity.

c. **A subcontractor** that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

Business Associate **does not** include:

a. A health care provider, with respect to disclosures by a Covered Entity to the health care provider concerning the treatment of the individual.

b. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) (meaning the Business Associate Agreement provisions) apply and are met.

c. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

d. A Covered Entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (*A-a in this definition*) for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (*A-b in this definition*) of this definition to or for such organized health care arrangement by virtue of such activities or services.

B **Patient safety activities** means the following activities carried out by or on behalf of a Patient Safety Organization (PSO) or a provider:

1. Efforts to improve patient safety and the quality of health care delivery;

2. The collection and analysis of patient safety work product;

3. The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;

4. The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;

5. The maintenance of procedures to preserve confidentiality with respect to patient safety work product;

6. The provision of appropriate security measures with respect to patient safety work product;

7. The utilization of qualified staff; and

8. Activities related to the operation of a patient safety evaluation system (the collection, management, or analysis of information for reporting to or by a Patient Safety Organization) and to the provision of feedback to participants in a patient safety evaluation system.

C **Data aggregation**, is where a Business Associate in its capacity as the Business Associate of one Covered Entity combines the PHI of such Covered Entity with PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity in order to permit the creation of data for analyses that relate to the health care operations of the respective covered entities.

D **Disclosure** means the release, transfer provision of access to, or divulging in any manner of information outside the entity holding the information.

E **Subcontractor** means a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

F **Organized health care arrangement** means:

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

2. An organized system of health care in which more than one Covered Entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint activities that include at least one of the following:

   - Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

   - Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

   - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

PROCEDURES

1. The Privacy & Security Officer or designee will identify and retain a list of updated Business Associates of the Plan.

2. The Privacy & Security Officer will utilize the Plan's Business Associate Agreement which was developed in compliance with the HIPAA Rules at 164.504(e) and the 2013 HIPAA Omnibus regulations and approved by the Plan's legal counsel.

3. The Privacy & Security Officer or their designee will manage the process and make a good faith effort in assuring that the Plan has a valid signed Business Associate Agreement with each existing and new Business Associate within the timeframes outlined in the regulations.

4. The Privacy & Security Officer or their designee will follow-up with Business Associates on an ongoing basis to review the status of any **unsigned** Business Associate Agreements.

5. If Business Associates have questions regarding Business Associate Agreement language, the Business Associate will be referred to the Privacy & Security Officer or the Plan's legal counsel.

6. When a Business Associate returns an executed copy of the Business Associate Agreement, the Privacy & Security Officer will retain the signed copy and make available to the Plan upon request.

7. Workforce Members who identify a breach of contract by a Business Associate, such as an issue noted in paragraph D of the policy section of this document, should report the breach to the Privacy & Security Officer. Privacy & Security Officer will consult with Legal Counsel to address it with the Business Associate in writing. The Privacy & Security Officer will take steps to document contact with the Business Associate regarding the breach and seek assurance from the Business Associate that protocol is in place to prevent further breach.

8. The Privacy & Security Officer will retain documentation of Business Associate Agreement and discussion of any breach, as required by the Plan's Policy on Record Retention.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 160.103, 164.502(e), 164.504, 164.532, 164.314(a), and 164.314(a)(2)(iii).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy.

- **FOR PUBLIC HEALTH ACTIVITY,**
- **FOR VICTIMS OF ABUSE, NEGLECT OR DOMESTIC VIOLENCE,**
- **FOR HEALTH OVERSIGHT ACTIVITIES,**
- **FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS (e.g. SUBPOENA),**
- **FOR LAW ENFORCEMENT PURPOSES (e.g. DECEASED, CORONER, FUNERAL DIRECTOR, ORGAN PROCUREMENT, ETC.),**
- **FOR RESEARCH,**
- **TO AVERT A THREAT TO HEALTH OR SAFETY,**
- **FOR SPECIALIZED GOVERNMENT FUNCTIONS (e.g. National Security, Inmates),**
- **FOR WORKER'S COPENSATION.**

POLICY STATEMENT

This policy and procedure is adopted pursuant to Sections 164.502(a)(5)(iii) and 164.512 of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and 42 CFR Part 2 and their implementing regulations and guidance. If the Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

Subject to the restrictions listed below on disclosing PHI related to substance, use and disorder ("SUD") records protected under 42 USC § 290dd-2 and 42 CFR Part 2 (collectively "Part 2"), the Plan and its Business Associates may use and disclose PHI as required by the law and for Public Health Activity, Victims of Abuse, Neglect or Domestic Violence, Health Oversight Activities, Judicial and Administrative Proceedings, Law Enforcement, Research, to Avert a Serious Threat to Health or Safety, or for Specialized Government Functions purposes **without the written authorization of the individual who is the subject of the information and the Plan is not required to give the individual the opportunity to agree or object to the use or disclosure**.

1) Restrictions on disclosing PHI related to substance use disorder:

a. The restriction on use and disclosure of substance use disorder apply to any records which:

a) Would identify a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person; and

b) Contain substance use disorder information obtained by a federally assisted substance use disorder program after March 20, 1972 (Part 2 Program), or contain alcohol use disorder information obtained by a federally assisted alcohol use disorder or substance use disorder program after May 13, 1974 (Part 2 program);

or if obtained before the pertinent date, is maintained by a Part 2 Program after that date as part of an ongoing treatment episode which extends past that date; for the purpose of treating a substance use disorder, making a diagnosis for that treatment, or making a referral for that treatment.

b. Except as otherwise authorized by a court order or by the consent of the patient, a record referred to in paragraph 2)a), or testimony relaying the information contained therein, may not be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any Federal, State, or local authority, against a patient including with respect to the following activities:

a) Such record or testimony shall not be entered into evidence in any criminal prosecution or civil action before a Federal or State court.

b) Such record or testimony shall not form part of the record for decision or otherwise be taken into account in any proceeding before a Federal, State, or local agency.

c) Such record or testimony shall not be used by any Federal, State, or local agency for a law enforcement purpose or to conduct any law enforcement investigation.

d) Such record or testimony shall not be used in any application for a warrant.

c. Permitted Disclosure:

a) Consent – the following shall apply with respect to the contents of any record referred to in paragraph 2)a):

(1) Such contents may be used or disclosed in accordance with the prior written consent of the patient with respect to whom such record is maintained.

(2) Once prior written consent of the patient has been obtained, such contents may be used or disclosed by a covered entity, business associate, or a program subject to this section for purposes of treatment, payment, and health care operations as permitted by the HIPAA regulations. Any information so disclosed may then be redisclosed in accordance with the HIPAA regulations.

(3) It shall be permissible for a patient's prior written consent to be given once for all such future uses or disclosures for purposes of treatment, payment, and health care operations, until such time as the patient revokes such consent in writing.

b) Without Consent – whether or not the patient, with respect to whom any given record referred to in paragraph 2)a) is maintained, gives written consent, the content of such record may be disclosed as follows:

(1) To medical personnel to the extent necessary to meet a bona fide medical emergency.

(2) To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such

personnel may not identify, directly or indirectly, any individual patient in any report of such research, audit, or evaluation, or otherwise disclose patient identities in any manner.

(3) If authorized by an appropriate order of a court of competent jurisdiction granted after application showing good cause therefor, including the need to avert a substantial risk of death or serious bodily harm. In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services. Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure.

(4) To a public health authority, so long as such content meets the standards established in Section 164.514(b) of title 45, Code of Federal Regulations (or successor regulations) for creating de-identified information.

Uses And Disclosures Required By Law:

Subject to the restrictions for uses and disclosures of SUD records, the Plan may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. "Required by law" means a mandate in law enforceable in court that compels an entity to disclose PHI, and not just a covered entity. The Plan must meet the requirements (described below) for:

- victims of abuse, neglect or domestic violence;
- judicial and administrative proceedings; and
- law enforcement purposes.

Disclosures For Public Health Activity:

Subject to the restrictions for uses and disclosures of SUD records, the Plan may use or disclose PHI for the public health activities and purposes noted below:

a. to a public health authority authorized by law to collect or receive PHI **for the purpose of preventing or controlling disease, injury or disability**. This includes but is not limited to the following:

- Reporting disease or injury;
- Reporting vital events such as birth or death;
- Conducting public health surveillance, investigations or interventions; or
- At the direction of a public health authority to an official of a foreign government agency that is acting in collaboration with a public health authority.

b. to a public health authority or other appropriate government authority authorized by law to receive **reports of child abuse or neglect**.

c. to a person subject to the **jurisdiction of the Food and Drug Administration (FDA)** with respect to an FDA-related product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

- To collect or report adverse events, product defects or problems or biological product deviations;
- To track FDA-regulated products;
- To enable product recalls, repairs or replacement or look back (locating and notifying individuals who have received products that have been recalled, withdrawn or are the subject of the look back); or
- To conduct post-marketing surveillance.

d. to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition if the Plan or public health authority is authorized by law to notify such person as necessary to conduct a public health intervention or investigation.

e. to an employer about an individual who is a member of the workforce of the employer if the covered entity is a covered health care provider who provides health care to the individual at the request of the employer to conduct an evaluation relating to **medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury**.

- The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance.
- The employer needs such findings in order to comply with its obligations under 29 C.F.R. 1904-1928 (Recording and reporting occupational injuries and illnesses), 30 C.F.R. parts 50-90 (Mine safety and health) or State law.
- The covered health care provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the health care is provided or if the health care is provided on the worksite, by posting the notice in a prominent place at the location where the health care is provided.

f. to a school about an individual who is a student or prospective student of the school if the Protected Health Information this is disclosed is **limited to proof of immunization**, the school is required by State or other law to have such proof of immunization prior to admitting the individual and the covered entity obtains and documents the agreements to this disclosure from either a parent, guardian or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or the individual, if the individual is an adult or emancipated.

Disclosures For Victims Of Abuse, Neglect Or Domestic Violence:

Except for reports of child abuse or neglect (as discussed above under Public Health Activity, letter b), the Plan may disclose PHI about an individual whom the Plan reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence. Disclosure will be made only:

a. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of the law;

b. If the individual agrees to the disclosure; or

c. To the extent the disclosure is expressly authorized by statute or regulation and the Plan, in the exercise of professional judgment, believes the disclosure is necessary to prevent further harm to the individual (victim) or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

The Plan will promptly inform an individual of any disclosure noted above unless the Plan believes that informing the individual would place the individual at risk of serious harm, or if the Plan would be informing a personal representative who the Plan believes is responsible for the abuse or injury and informing the representative would not be in the best interests of the individual.

Disclosures For Health Oversight Activities:

The Plan may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative or criminal proceedings or actions or other activities necessary for appropriate oversight of:

a. the health care system;

b. government benefit programs for which health information is relevant to beneficiary eligibility;

c. entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

d. entities subject to civil rights laws for which health information is necessary for determining compliance.

Health oversight activity does not include (and the Plan will not disclose PHI for) an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

- receipt of health care;
- a claim for public benefits related to health; or

- qualification for or receipt of public benefits or services when a patient's health is integral to the claim for public benefits or services.

Disclosure For Judicial And Administrative Proceedings (e.g. subpoena):

Subject to the restrictions for uses and disclosures of SUD records, the Plan may disclose PHI in the course of any judicial or administrative proceeding as follows:

a. in response to **an order of a court** or administrative tribunal (provided that the Plan discloses only the PHI expressly authorized by such order); or

b. in response to a **subpoena**, discovery request or other lawful process that is **not** accompanied by an order of the court or administrative tribunal, if:

- the Plan receives "satisfactory assurance" from the party seeking PHI that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request in accordance with the definition of satisfactory assurance in compliance with Section 164.512 (e)(1) (iii) that:
    - the individual has been given notice of the request and the Plan receives from that party a written statement and accompanying documentation demonstrating that the party requesting the PHI has made a good faith attempt to provide written notice to the individual (or mail to the last known address); and
    - the Notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and the time for the individual to raise objections to the court or administrative tribunal has elapsed and no objections were filed or all objections filed by the individual have been resolved by the court or administrative tribunal and the disclosures being sought are consistent with such resolution; or
- The Plan receives "satisfactory assurance" from the party seeking the PHI that reasonable efforts have been made by the party to secure a "qualified protective order" (as defined below), if;
    - the Plan receives from the party a written statement and accompanying documentation demonstrating that the parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
    - the party seeking the PHI has requested a "qualified protective order" from such court or administrative tribunal.

Disclosure For Law Enforcement Purposes:

Subject to the restrictions for uses and disclosures of SUD records, the Plan may disclose PHI for a law enforcement purpose to a law enforcement official if the following conditions are met:

a. As required by law(s) that require reporting of certain types of wounds or other physical injuries;

b. In compliance with and as limited by the requirements of:

- a court order or court-ordered warrant;
- a subpoena or summons issued by a judicial officer;
- a grand jury subpoena; or
- an administrative request, for which response is required by law, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process under law provided that the PHI sought is relevant to a legitimate law enforcement inquiry, the request is specific and limited to the purpose for which the information is sought, and de-identified information could not be used.

c. The Plan may disclose PHI about an individual in response to a law enforcement official's request for such information **for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person**, but the Plan may disclose only the following information:

- Name and address;
- Date and place of birth;
- Social security number;
- ABO blood type and Rh factor (if known);
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

The Plan may not disclose for the purposes of identification or location, any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

d. The Plan may disclose PHI in response to a law enforcement official's request about an individual who is (or is suspected to be) **a victim of a crime** if:

- The individual agrees to such disclosure, or
- The Plan is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
    - the law enforcement official represents that the PHI is needed to determine whether a violation of law by someone other than the victim has occurred, and that such information is not intended to be used against the victim, that immediate law enforcement activity which depends upon the disclosure would be materially and

adversely affected by waiting until the individual is able to agree to the disclosure, and

- that the disclosure of PHI is in the best interest of the individual.

e. The Plan may disclose **PHI about an individual who has died** to a law enforcement official if the Plan suspects the individual's death may have resulted from criminal conduct.

f. The Plan may disclose to a law enforcement official PHI that the Plan believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

g. The Plan may disclose PHI to a coroner or medical examiner for the purpose of identification of a deceased person, determining a cause of death, or other duties as authorized by law.

h. The Plan may disclose PHI to funeral directors as necessary to carry out their duties with respect to a deceased individual or if necessary, PHI may be disclosed prior to and in anticipation of the individual's death.

i. The Plan may disclose PHI to **organ procurement organizations** or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

Disclosure For Research Purposes:

The Plan may provide PHI for research (regardless of the source of funding for the research) if:

- The Plan obtains an alteration to or waiver of the authorization for use or disclosure of PHI that has been approved by an Institutional Review Board (IRB) or a privacy board (as defined in 164.512(I)(1)(B).

- The Plan must also receive representation from the researcher(s) that use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or similar purpose, and that no PHI will be removed from the Plan by the researcher in the course of the review, and the PHI is necessary for research purposes.

- **Research on decedents**: The Plan must obtain from the researcher representation that the use and disclosure is solely for research on the PHI of decedents, documentation of the death of such individuals and representation that the PHI is necessary for research purposes.

- **Waiver of Authorization:** For use and disclosure of PHI to be permitted based on documentation or approval of an alteration or waiver of authorization, the documentation must include all the following:

    - A statement identifying the IRB or privacy board and the date the alteration or waiver was approved.

    - A statement that the IRB or privacy board has determined that the alteration or waiver of authorization satisfies the following criteria:

a. use or disclosure of PHI involves no more than minimal risk to the privacy of individuals based on at least the presence of an adequate plan to protect the identifiers from improper use and disclosure;

b. an adequate plan to destroy the identifiers at the earliest opportunity; and

c. written assurance that the PHI will not be reused or disclosed except as required by law, for authorized oversight of the research study.

- The research could not practically be conducted without the waiver or alteration and could not be conducted without access to the PHI.

- A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board.

- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures in compliance with 164.512 (i) (2)(iv).

- Documentation of the alteration or waiver of authorization must be signed by the chair or other member as designated by the chair of the IRB or privacy board.

Disclosure To Avert A Serious Threat To Health Or Safety:

The Plan may (consistent with applicable law and standards of ethical conduct) use and disclose PHI if the Plan, in good faith, believes the use or disclosure:

- Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person(s) reasonably able to prevent or lessen the threat or

- Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

The Plan CANNOT disclose PHI relating to an individual's therapy or request for therapy to treat a propensity to commit the criminal conduct that is the basis for the disclosure (164.512 (j)(2)).

When the Plan can disclose PHI, such information is to be limited (in accordance with 164.512 (f)(2)(i)) that indicates the Plan may only disclose the following:

a. Name and address;

b. Date and place of birth;

c. Social security number;

d. ABO blood type and Rh factor;

e. Type of injury;

f. Date and time of treatment;

g. Date and time of death, if applicable; and

h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

The Plan may not disclose for the purposes of identification or location any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

Disclosures For Specialized Government Functions (e.g. National Security):

a. The Plan may disclose PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the military authority has published in the *Federal Register* the appropriate military command authorities; and the purposes for which the PHI may be used or disclosed.

b. The Plan may disclose PHI to authorized Federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq*.) and implementing authority (e.g., Executive Order 12333). The Plan may also disclose PHI to officials for the protection of the President or other persons or to foreign heads of state 164.512 (k)(3).

c. The Plan may disclose PHI to Correctional Institutions and other law enforcement custodial situations having lawful custody of an inmate or other PHI of an inmate or individual if the correctional institution or law enforcement official represents that such PHI is necessary for:

- The provision of health care to such individual;
- The health and safety of such individual or other inmates;
- The health and safety of the officers or employees of or others at the correctional institution or those persons responsible for the transporting of inmates or their transfer from one institution, facility or setting to another;
- Law enforcement on the premises of the correctional institution; or
- The administration and maintenance of the safety, security and good order of the correctional institution.

An individual is no longer an inmate when released on parole, probation, supervised release or otherwise is no longer in lawful custody.

d. A health plan that is a state or local government program providing public benefits may disclose PHI relating to eligibility or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies (or the maintenance of such information in a single or combined data system accessible to all such government agencies) is authorized by statute or regulation, is necessary to coordinate the covered functions of such programs, or is necessary to improve management of such programs.

Workers' Compensation 164.512 (l):

The Plan may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

Federally Assisted means a program that:

- Is conducted in whole or in part, whether directly or by contract or otherwise by any department or agency of the United States, except as set forth in 42 CFR 2.12(c).
- Is being carried out under license, certification, registration, or other authorization granted by any department or agency of the United States including but not limited to:
    - Participating provider in the Medicare program;
    - Authorization to conduct maintenance treatment or withdrawal management; or
    - Registration to dispense a substance under the Controlled Substances Act to the extent the controlled substance is used in the treatment of substance use disorder.
- It is supported by funds provided by any department or agency of the United States by being:
    - A recipient of federal financial assistance in any form, including financial assistance which does not directly pay for the substance use disorder diagnosis, treatment, or referral for treatment; or
    - Conducted by a state or local government unit which, through general or special revenue sharing or other forms of assistance, receives federal funds which could be (but are not necessarily) spent for the substance use disorder program; or
- It is assisted by the Internal Revenue Service of the Department of the Treasury through the allowance of income tax deductions for contributions to the program or through the granting of tax exempt status to the program.

- **Satisfactory assurance means** (in compliance with 164.512 (e) (1) (iii) that the Plan receives from the party a written statement and accompanying documentation that the party requesting such information has made a good faith attempt to provide written notice to the individual, the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and the time for the individual to raise an objection has elapsed and no objections were filed or all objections filed have been resolved by the court or administrative tribunal and disclosures are consistent with such resolution.

- **Qualified protective order means** (in compliance with 164.512 (e) (1) (v)) an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing PHI for any purpose other than the litigation or proceeding for which such information was requested; or requires the return to the

covered entity or destruction of the PHI, including copies made, at the end of the litigation or proceeding.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates are required to implement procedures on behalf of the Plan and shall implement procedures, for uses and disclosures of PHI in compliance with Sections 164.502(a)(5)(iii) and 164.512 of the HIPAA Rules and 42 CFR Part 2. Such procedures must provide that PHI disclosed without the authorization of the individual must be in compliance with the HIPAA Rules and disclose only the minimum necessary. In addition, disclosures must be documented in accordance with the Plan's policy on Record Retention. Copies of such procedures will be provided to the Plan upon request.

The Plan's legal counsel may be consulted when a subpoena, discovery request, or other lawful process is received.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Sections 164.502(a)(5)(iii) and 164.512.
- 42 CFR Part 2
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy.

POLICY STATEMENT

While the Plan acknowledges that there are State and Federal record retention requirements for specific types of information (i.e., financial, personnel, trade/service mark, OSHA, Fair Labor Standards, IRS, Civil Rights Act and Equal Pay Act, etc.) this policy and procedure is drafted to provide guidance to this Plan on record retention in order to comply with the HIPAA Rules.

This policy and procedure is adopted pursuant to Sections 164.530(j), 164.528, 160.310(a) and various other sections and requirements of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan acknowledges that it must:

a. Maintain the HIPAA policies and procedures in written or electronic form;

b. If a communication, action, activity, or designation is required by the Privacy regulation such communication, action, activity, or designation documentation must be maintained in writing or electronic copy.

Provide records and compliance reports. The Plan must keep such records and submit such compliance reports, in such time and manner and containing such information, as the HHS Secretary may determine to be necessary to enable the Secretary to ascertain whether the Plan has complied or is complying with the applicable requirements of the applicable standards, requirements, and implementation of the HIPAA Rules.

In compliance with 164.528 the Plan will retain proof of its accounting of disclosures of PHI for the six years prior to the date on which the accounting was requested, except for disclosures:

- To carry out treatment, payment and health care operations as provided in § 164.506;
- To individuals of PHI about them as provided in § 164.502;
- Pursuant to an authorization as provided in § 164.508 (however signed authorizations will be retained);
- To persons involved in the individual's care or other notification purposes as provided in § 164.510;
- For national security or intelligence purposes as provided in § 164.512(k)(2);
- To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);
- That occurred prior to the compliance date for this Plan as Covered Entity.

Record Retention Period Policy. The Plan will comply with the HIPAA Rules required documentation must be retained (either in written or electronic form) **for the later of six years from the date it was created or the date it was last in effect**.

Cooperate with complaint investigations and compliance reviews. A Covered Entity or Business Associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the Covered Entity or Business Associate to determine whether it is complying with the applicable administrative simplification provisions.

Permit access to information.

1. A Covered Entity or Business Associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a Covered Entity or Business Associate must permit access by the Secretary at any time and without notice.

2. If any information required of a Covered Entity or Business Associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the Covered Entity or Business Associate must so certify and set forth what efforts it has made to obtain the information.

3. PHI obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

1. **Record** means an item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for this Plan as a Covered Entity. Record **does not** include:

    a. Education records relating to a student or as maintained by an educational agency or institution or by a person acting for such agency or institution covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g and what is not an education record at 20 U.S.C. 1232g(a)(4)(B)(iv);

    b. Employment records held by this Plan (a Covered Entity) in its role as employer. Employment records (while not officially defined by the Privacy Regulations), under this policy and procedure means information needed by this employer to facilitate FMLA requests, sick leave requests, drug screening programs, fitness-for-duty exams, OSHA requirements and other similar programs. Health information that is received by this employer in its employment capacity is not PHI and therefore not a record as defined in this policy.

2. **Electronic media** means:

    a. Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

    b. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

PROCEDURES

The Plan's Business Associates have been delegated the responsibility to retain documentation and to implement procedures, in compliance with Section 164.530(j), 164.528, 160.310(a) of the HIPAA Rules, on behalf of the Plan. Copies of such procedures and record retention documentation will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.530(j), 164.528, 160.310(a).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy

HIPAA POLICY AND PROCEDURE FOR USE AND DISCLOSURE OF PHI REQUIRING AN OPPORTUNITY FOR AN INDIVIDUAL TO AGREE OR OBJECT

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.510(b) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), the Plan will follow the revised rules.

The Plan may use or disclose PHI, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with applicable requirements of this policy. The Plan may verbally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure of PHI permitted by this policy.

Uses and disclosures of PHI for involvement in the individual's care and notification purposes:

The Plan may disclose to a family member, other relative, or a close personal friend of an individual, or to any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care. This disclosure can only be made according to the Plan's Procedure described below.

The Plan may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with this policy.

In addition, the Plan may disclose a deceased individual's PHI to family member, other relative or close personal friend of the deceased individual or any other person previously identified by the deceased individual to the Plan if the disclosure is directly relevant to such person's involvement with the deceased individual's care or payment related to the deceased individual's health care, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the Plan. The Plan will comply with the terms of this policy and procedure with respect to the PHI of a deceased individual for a period of 50 years following the date of death. After 50 years has passed, the individually identifiable health information of the deceased individual is no longer considered to be PHI that is protected by the HIPAA Rules.

Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, the Plan may use or disclose the PHI if it:

- Obtains the individual's agreement;
- Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
- Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

Limited uses and disclosures when the individual is not present.

If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Plan may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes. The Plan may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

If the individual is deceased, a Covered Entity may disclose to a family member, or other persons who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Covered Entity.

Use and disclosures for disaster relief purposes.

The Plan may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosure of PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. These requirements apply to such uses and disclosure to the extent that the Plan, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates are responsible for implementing procedures in compliance with HIPAA Privacy requirements on behalf of the Plan and to allow individuals to agree or object to certain uses and disclosures of PHI in compliance with Section 164.510(b) of the HIPAA Rules. Copies of such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.510
- The Plan's Privacy & Security Officer

HIPAA POLICY AND PROCEDURE ON COMPLAINTS

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(d), 164.306, 164.310(b) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

In compliance with Section 164.530(d), the Plan, through its Business Associates, has provided a process for individuals to make complaints concerning the Plan's Privacy policies and procedures or the requirements of the HIPAA Rules. Further, the Plan, through its Business Associates, will document complaints and the disposition of complaints.

Complaints to the Secretary of HHS: In compliance with Section 164.306, the Plan acknowledges that a person who believes the Plan or its Business Associate is not complying with the applicable requirements of the standards, requirements, and implementation specifications of the Privacy regulations may file a complaint with the Secretary of HHS.

Complaints under this section must meet the following requirements:

- A complaint must be filed in writing, either on paper or electronically.
- A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable standards, requirements, and implementation specifications of the Privacy regulation.
- A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, (unless this time limit is waived by the Secretary for good cause shown).
- The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.
- The Secretary may investigate complaints and such investigation may include a review of the pertinent policies, procedures, or practices of the Plan and of the circumstances regarding any alleged acts or omissions concerning compliance.

Investigation of Complaints by the Secretary of HHS: In compliance with Section 164.310(b) the Plan will cooperate with the Secretary of the Department of Health and Human Services (HHS), if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the Plan to determine whether it is complying with the applicable standards, requirements, and implementation specifications of the Privacy regulation.

The Secretary will investigate any complaint filed under this Section 160.306 when a preliminary review of the facts indicates a possible violation due to willful neglect.

- The Secretary may investigate any other complaint filed under this section.

- An investigation under this section may include a review of the pertinent policies, procedures, or practices of the Covered Entity or Business Associate and of the circumstances regarding any alleged violation.

- At the time of the initial written communication with the Covered Entity or Business Associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

In accordance with Section 160.308, the Secretary will conduct a compliance review to determine whether a Covered Entity or Business Associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

The Secretary may conduct a compliance review to determine whether a Covered Entity or Business Associate is complying with the applicable administrative simplification provisions in any other circumstance.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Privacy & Security Officer is designated as the individual responsible for overseeing the complaint process. The Plan accepts and will investigate complaints of violations of the Plan's privacy policies and procedures from covered individuals as well as complaints from Business Associate's staff. The Privacy & Security Officer will determine:

- Whether there has been a violation of the Plan's privacy policies and procedures,

- The seriousness and effect of the violation, and

- Any corrective action that may be taken.

All complaints received and the outcome of the investigation shall be documented in accordance with the Record Retention policy.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR 164.530(d), 164.306, 164.310(b).

- The Plan's Privacy & Security Officer.

- See also the policy/procedure in this Manual on "Notification in Case of Breach" and Record Retention Policy

HIPAA POLICY AND PROCEDURE FOR DE-IDENTIFICATION AND RE-IDENTIFICATION OF PHI

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514 and 502(d) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and Guidance Regarding Methods for De-identification of PHI in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule dated November 26, 2012. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

1. **De-identification:** The Plan, through its Business Associates, may disclose health information that it has determined does not contain individually identifiable information by removing the 18 identifiers from the information it uses or obtains. To determine that information it discloses does not contain individually identifiable health information it must follow one of the following methods.

    a. A person with knowledge of generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that:

    - the risk is very small that the information disclosed could be used, alone or in combination with other reasonably available information, to identify an individual who is a subject of the information; and
    - applies methods to mitigate risk
    - The Plan documents the methods and the result of the analysis that justify this determination.
    - If this procedure is used, the expert will comply with the guidance set forth in the Guidance Regarding Methods for De-identification of PHI in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule dated November 26, 2012.

or, the safe harbor method:

    b. The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed, and the Plan does not have knowledge that the information provided could be used alone or in combination with other information to identify an individual who is a subject of the information:

    (1) **Names**;

    (2) **All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip codes**.

    - The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census,

(http://www.census.gov/) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people.

- If the geographic units that make up the initial three digits of a zip code contain 20,000 or fewer people, the first three digits must be changed to 000.

- Utilizing Census 2000 data, zip codes with the following initial three digits must have the zip code changed to 000: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, 893.

(3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

- For example, de-identified information could not include the day and month of a medical procedure or event (i.e., 1/1/2009), but it may include only the year (i.e.2009).

- Age may be included in de-identified information except that age over 89 must **be indicated as "90 or above"** whether the actual age is stated or implied (i.e., if the birth year is 1910 and treatment is provided in 2010, the birth year must be reported as "on or before 1920."

(4) **Telephone numbers**;

(5) **Fax numbers**;

(6) Electronic mail **(e-mail) addresses**;

(7) **Social security numbers** (SS#);

(8) **Medical record numbers**;

(9) **Health plan beneficiary numbers**;

(10) **Account numbers**;

(11) **Certificate/license numbers**;

(12) **Vehicle identifiers and serial numbers, including license plate numbers**;

(13) Device identifiers and serial numbers;

(14) Web Universal Resource Locators (URLs);

(15) **Internet Protocol (IP) address numbers**;

(16) **Biometric identifiers, including finger and voice prints**;

(17) **Full face photographic images and any comparable images**; and

(18) Any other unique identifying number, characteristic, or code, except as permitted for re-identification of the data as described below. For example, a unique identifier could be that the individual is the "current President of the University" or a clinical trial number.

Parts or derivatives of any of the above listed identifiers may not be included in de-identified information. For example, de-identified information <u>may not include</u> the last four digits of the individual's social security number or the individual's initials.

2. **Re-identification:** The Plan may assign a code or other means of record identification to allow information de-identified to be re-identified by the Plan provided that:

   a. The code or other means of record identification is not derived from or related to the individual; and

   b. The code or other means cannot be translated so as to identify the individual; and

   c. The Plan does not use or release the code or other means of record identification for any other purpose; and

   d. The Plan does not disclose the mechanism for re-identification.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **De-identified** means health information that does not identify an individual and which the Plan believes there is no reasonable basis that the information can be identified. De-identified information is not individually identifiable health information.

- **Re-identified** means assignment of a code or other means of record identification to allow the identification of the original identity that was de-identified.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates that are required to implement procedures on behalf of the Plan, in compliance with Sections 164.514 and 164.502(d) of the HIPAA Rules, shall implement procedures for de-identification and re-identification of PHI. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.514, 164.502(d)

- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE ON SANCTIONS FOR VIOLATION OF HIPAA RULES

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(e), and to the extent applicable, 164.308(a)(1)(ii)(C), of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

The Plan and its Business Associates must have and apply appropriate sanctions against members of its workforce who fail to comply with their respective HIPAA policies and procedures of the Plan or the requirements of the HIPAA Rules. The respective entity must document the sanctions that are applied, if any.

A Workforce Member of the Plan who is responsible for handling PHI of covered individuals will be sanctioned for violating the HIPAA Rules and the HIPAA policies and procedures adopted by the Plan. However, the Plan or Business Associate will not impose sanctions on whistleblowers or members of its workforce who are victims of a crime as those terms are defined elsewhere in these policies and procedures.

The Privacy & Security Officer and/or other Business Associate will determine whether there has been a violation of the HIPAA Rules, the seriousness and effect of the violation and the sanction to be imposed on the covered individual.

The Privacy & Security Officer and/or other Business Associate have discretion to determine appropriate sanctions for violation of the HIPAA Rules. Sanctions will include disciplinary action up to and including dismissal of the Workforce Member.

Sanctions will not be imposed for disclosure of PHI that meets the conditions set out in Sections 164.530(g)(2) of the HIPAA Rules regarding whistleblower protections.

KEY DEFINITIONS

Under this Plan, sanction refers to the ramifications on an individual for breaking Plan policies related to HIPAA Privacy and Security. For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

Any possible sanction due to a violation of the HIPAA Rules by a member of the Board of Trustees will be coordinated between the Privacy & Security Officer and Legal Counsel for the Plan.

Business Associates shall implement procedures, in compliance with Section 164.530(e) and 164.308(a)(1)(ii)(C) of the HIPAA Rules, addressing sanctions imposed on their respective Workforce Members that violate the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Breach.

ADDITIONAL RESOURCES

- 45 CFR Section 164.530(e) and 164.308(a)(1)(ii)(C)
- The Plan's Privacy & Security Officer

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(b) and, to the extent applicable, 164.308(a)(5)(i) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

The Plan must train all members of its workforce (which is the Board of Trustees for the Plan and any Fund employees) on the policies and procedures with respect to PHI required by the HIPAA Rules, as necessary and appropriate for the members of the workforce to carry out their function as a Plan Sponsor. This training must meet the following requirements:

a. To each new Trustee within a reasonable period of time after the person joins the Joint Board of Trustees and on an ongoing basis; and

b. To each Trustee whose functions are affected by a material change in the policies or procedures required by the HIPAA Privacy Regulation or the procedures of this Plan, within a reasonable period of time after the material change becomes effective.

c. The Plan must document that the training, as described above, has been provided.

Therefore, it is the policy of the Plan to train Trustees on all Plan policies and procedures concerning the use or disclosure of PHI implemented for compliance with the HIPAA Rules.

Business Associates (including the Fund Administrator) are responsible, as applicable, for implementing policies and procedures to train their respective Workforce Members.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Workforce Member(s)** means Trustees, employees, volunteers, trainees and other persons whose conduct, in the performance of work for the Plan, is under the direct control of the Plan, Administrative Office and/or Business Associates whether or not they are paid by the Plan, the Administrative Office or the Business Associate

PROCEDURES

The Privacy & Security Officer will be responsible for coordinating Trustees training on the Plan's HIPAA policies and procedures as follows:

a. Within a reasonable period after the person joins the Board of Trustees and on an ongoing basis

b. To each Trustee whose functions are affected by a material change in the policies or procedures required by the HIPAA Privacy Regulation or the procedures of this Plan, within a reasonable period of time after the material change becomes effective.

The Privacy & Security Officer, on behalf of the Plan, will document the training, as described above.

Business Associates will be responsible for implementing procedures, in compliance with Section 164.530(b) and 164.308(a)(5)(8) of the HIPAA Final Rules, for training workforce members. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR 164.530(b) and 164.308(a)(5)(i)
- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE FOR USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS (TPO)

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(a) and Section 164.506 of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and 42 CFR Part 2 and their implementing regulations and guidance. If the Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

General Rule: Pursuant to Section 164.502(a), the Plan (as a Covered Entity) or a Business Associate may not use or disclose PHI, except as permitted or required by HIPAA and in compliance with the HIPAA Policy and Procedure for Minimum Necessary. The Plan is permitted to use or disclose PHI as follows:

1. **To the individual**;

2. For **treatment, payment, or health care operations (TPO),** as permitted by and in compliance with the HIPAA Rules and 42 CFR Part 2 on uses and disclosures of PHI to carry out TPO.

3. Incident to a use or disclosure otherwise permitted or required by 45 CFR Part 164, Subpart E, provided that the Covered Entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

4. Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in accordance with a signed valid **authorization or consent** (that complies with 164.508 and 42 CFR Part 2 as outlined in the Plan's policy on Use of Authorizations & Consents.)

    a) For uses and disclosures requiring an opportunity for the individual to agree or to object pursuant to § 164.510; and

    b) As permitted by an in compliance with any of the following:

        i) Section 164.502

        ii) Section 164.512.

        iii) Section 164.514(e), (f), or (g).

    c) The Plan is required to disclose PHI:

    d) To the individual, when requested under, and required by § 164.524 or § 164.528; and

    e) When required by the Secretary to investigate or determine the Plan's compliance with 45 CFR Part 164, Subpart E.

5. Business Associate's Permitted uses and disclosures. A Business Associate may use or disclose PHI only as permitted or required by its Business Associate Agreement or as required by law. The Business Associate may not use or disclose PHI in a manner that would violate the requirements of the HIPAA

Rules or 42 CFR Part 2, if done by the Covered Entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its Business Associate Agreement.

6. Business Associate's Required Uses and Disclosures. A business Associate is required to disclose PHI:

   a) When required by the Secretary under 45 CFR Part 160, Subpart C to investigate or determine the Business Associate's compliance with the HIPAA Rules.

   b) To the Covered Entity, individual, or individual's designee, as necessary to satisfy a Covered Entity's obligation under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of PHI.

7. Prohibited Uses and Disclosures:

   a) Uses and disclosure of genetic information for underwriting purposes, in compliance with 45 CFR § 164.502(5)(i).

   b) Sale of PHI, except as set forth in 45 CFR § 164.502(5)(ii);

   c) Uses and disclosures of Part 2 records for civil, criminal, administrative, and legislative proceedings against the patient.

Permitted Uses and Disclosures to Carry out Treatment, Payment or Health Care Operations:

Pursuant to Section 164.506, except with respect to uses or disclosures that require an authorization (psychotherapy notes or marketing activities or sale of PHI with remuneration) or consent (substance, use and disorder records), the Plan may use or disclose PHI for treatment, payment, or health care operations (TPO) without obtaining consent or an authorization form. Use and disclosure of PHI must be consistent with other applicable requirements of HIPAA (such as minimum necessary) as described in the policies and procedures of the Plan.

Consent for Uses and Disclosures Permitted:

The Plan may obtain the consent of the individual to use or disclose PHI to carry out TPO. A voluntary consent document will not constitute valid permission to use or disclose PHI for a purpose that requires an authorization under the Privacy regulation (such as for psychotherapy notes or marketing or sale of PHI with remuneration as described in Section 164.508 of the Privacy regulation). (See also the policies and procedures entitled Use of Authorizations & Consents.)

Additionally a consent will not permit disclosure of PHI when another condition must be met for such use or disclosure to be permissible under HIPAA.

Treatment, Payment, or Health Care Operations:

1. The Plan may use or disclose PHI for its own TPO uses. The Plan may disclose PHI for treatment activities of a health care provider.

2. The Plan may disclose PHI to another Covered Entity or health care provider for the payment of the entity that receives the information.

3. The Plan may disclose PHI to another Covered Entity (such as another group health plan, health care provider or clearinghouse) for health care operations activities of the Covered Entity that receives the information, if the Plan and the other Covered Entity have or have a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for the purpose of:

    - Conducting quality assessment and improvement activities including patient safety activities; or

    - Reviewing the competence or qualifications of health care professionals, evaluating performance, conducting training programs, accreditation, certification, licensing, or credentialing activities; or

    - Health care fraud and abuse detection or compliance.

4. A Plan that participates in an organized health care arrangement (this term is defined below) may disclose PHI about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

Covered Entity means a:

- health plan,

- health care clearinghouse or

- health care provider who transmits any health information in electronic form in connection with a transaction covered by the transaction standards in 45 C.F.R. Part 162.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Payment means:

1. The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

2. The activities related to the individual to whom health care is provided and include, but are not limited to:

    a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

    b) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

c) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

d) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

e) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

f) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:

- Name and address;
- Date of birth;
- Social security number;
- Payment history;
- Account number; and
- Name and address of the health care provider and/or health plan

Health care operations means any of the following activities of the Plan to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

3. Underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable (§ 164.514(g) says that if a health plan receives PHI for the purpose of underwriting, enrollment, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such PHI for any other purpose, except as may be required by law);

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

6. Business management and general administrative activities of the Plan, including, but not limited to:

   a) Management activities relating to implementation of and compliance with the requirements of HIPAA;

   b) Customer service, including the provision of data analyses for policyholders, Plan Sponsors, or other customers, provided that PHI is not disclosed to such policy holder, Plan Sponsor, or customer.

   c) Resolution of internal grievances;

   d) The sale, transfer, merger, or consolidation of all or part of a Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and

   e) Creating de-identified health information, complying with minimum necessary rules, limited data sets, fundraising, underwriting and verification requirements of HIPAA for the benefit of the Plan.

Organized health care arrangement means:

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

2. An organized system of health care in which more than one Covered Entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint activities that include at least one of the following:

   - Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

   - Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

   - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk

3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

4. A group health plan and one or more other group health plans each of which are maintained by the same Plan Sponsor; or

5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

PROCEDURES

The Board of Trustees ("Trustees") is the Plan Sponsor and all Trustees and alternate Trustees thereof are designated as persons entitled to receive PHI for administration activities on behalf of the Plan. In general, potential PHI will be de-identified before being transmitted to Trustees or alternate trustees. If de-identification is not practical, the PHI shall be sent in non-electronic media such as fax, mail, messenger or phone. The Trustees use PHI as permitted for treatment, payment and health care operations "TPO" purposes, in accordance with the Plan Amendment. The Plan may disclose PHI to the Plan Sponsor for review of appeals of a benefit or for other reasons related to the administration of the Plan. The Plan will share the minimum information necessary to accomplish these purposes. The Trustees will not use PHI for employment or union-related actions or for any purpose unrelated to Plan administration. The Trustees will return or destroy all PHI received from the Plan in any form, and retain no copies of such PHI when no longer needed for the specified disclosure purpose. If return or destruction is not feasible, the Plan Sponsor will limit further uses and disclosures to those purposes that make the return or destruction infeasible.

Business Associates are required to implement procedures, in compliance with Sections 164.502(a) and 164.506 of the HIPAA Rules and 42 CFR Part 2, addressing uses and disclosures of PHI for treatment, payment and health care operations "TPO". Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Minimum Necessary and the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.502(a) and Section 164.506.
- 42 CFR Part 2
- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE FOR MITIGATION

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(f) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

In compliance with Section 164.530, the Plan will mitigate, to the extent practicable, any harmful effects known by the Plan of a use or disclosure of PHI in violation of the Plan's policies and procedures or HIPAA Rules by employees of the Plan or any Business Associate.

In order to mitigate harmful effects, the use or disclosure of PHI that violates the Plan's procedures and/or HIPAA must be known to the Plan. This means the Privacy & Security Officer must have been informed of the violation by an individual, a member of the Administrative Office's workforce, or a Business Associate. When mitigating harmful effects, the Plan will take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to an individual, and what steps can be taken to have a mitigating effect in that specific situation.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Mitigate** means to lessen or remove negative impacts.

PROCEDURES

The Trustees will notify the Privacy & Security Officer in a prompt manner of any known incidents relating to the use or disclosure of PHI. Business Associates shall implement procedures, in compliance with Section 164.530(f) of the HIPAA Rules to mitigate any harmful effects of PHI. Such procedures will be provided to the Plan upon request. Any use or disclosure of PHI by the Business Associate or their respective subcontractors that is not allowed by their Business Associate Agreements will be reported to the Privacy & Security Officer as outlined in their respective Business Associate Agreement.

1. The Privacy & Security Officer will document any notice that a use or disclosure of PHI by a Workforce Member or Business Associate is in violation of the Plan's policies and procedures or HIPAA Rules.

2. The Privacy & Security Officer will promptly initiate an investigation. The Privacy & Security Officer will also review the policy and procedure in this manual related to Breach. The Privacy & Security Officer reserves the right to contact legal counsel for assistance.

3. The Privacy & Security Officer will initiate a corrective action to attempt to prevent future similar disclosures.

4. If the PHI misuse involves a Workforce Member, the Privacy & Security Officer will reference the Plan's sanction policy for disciplinary action.

5. If the PHI misuse involves a Business Associate, the Privacy & Security Officer will:

    a. obtain a copy of the Plan's Business Associate Agreement.

    b. discuss the issue with the Business Associate and follow up in writing to document the conversation.

    c. ask the Business Associate for a corrective action plan.

    d. determine if the corrective action plan is appropriate and if not, work with the Business Associate to develop an acceptable corrective action plan.

    The Plan reserves the right to terminate a Business Associate Agreement if a mutually acceptable corrective action cannot be reached or the Plan finds that the Business Associate continues to misuse PHI despite notice by the Plan.

6. The Privacy & Security Officer will retain documentation of the mitigation issue, investigation and resolution in accordance with the Plan's record retention policy.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions and/or Breach.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.530(f).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy

HIPAA POLICY AND PROCEDURE REGARDING ANTI-RETALIATION

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530 (g) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

In compliance with Section 164.530, the Plan will not take retaliatory action against any person who files a complaint with the Plan or with the Department of Health and Human Services. The Plan and its Business Associates will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for exercising their rights under the HIPAA Rules or for filing or participating in filing a complaint under the complaint process established by the Plan or the Privacy regulations; or

2. Any individual or other person for filing a complaint with the Secretary of the Department of Health and Human Services under Subpart C of Section 160 of the HIPAA Rules; or

3. Any individual or other person for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act (relating to HIPAA Administrative Simplification, beginning with 42 U.S.C. § 1320d); or

4. Any individual or other person for opposing any act or practice made unlawful by HIPAA, provided the individual or person has a good faith belief that the practice opposed is unlawful and the manner of the opposition must be reasonable and not involve a disclosure of PHI in violation of HIPAA Rules. For example, an employee who discloses their own PHI to the media or a friend is not protected.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

As it relates to the Plan:

1. If the Privacy & Security Officer is notified of a **retaliatory action against an individual or other person the Privacy & Security Officer will** seek out the source of the person taking retaliatory action and educate them on the HIPAA Rules that prevent such action.

2. The Privacy & Security Officer may take other action as needed to adequately address the retaliatory action issue.

3. The Privacy & Security Officer will retain documentation of the investigation of the retaliatory action in accordance with the Plan's record retention policy and procedures.

As it relates to Business Associates:

Business Associates shall implement procedures, in compliance with Section 164.530(g) of the HIPAA Rules regarding anti-retaliation by its workforce members. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR Section 164.530 (g).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy

HIPAA POLICY AND PROCEDURE DISCLOSURES OF PHI BY WHISTLEBLOWERS AND VICTIMS OF CRIME

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(j) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

Disclosures by whistleblowers: The Plan is not considered to have violated the requirements of the Privacy regulation if a member of its workforce or a Business Associate discloses PHI provided that:

a) The workforce member or Business Associate believes in good faith that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Plan potentially endangers one or more patients, workers, or the public; and

b) The disclosure is to:

   i) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Plan or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Plan; or

   ii) An attorney retained by or on behalf of the workforce member or Business Associate for the purpose of determining the legal options of the workforce member or Business Associate with regard to the conduct described above.

Disclosures by workforce members who are victims of a crime: A Plan is not considered to have violated the requirements of the Privacy regulation if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official, provided that:

a) The PHI disclosed is about the suspected perpetrator of the criminal act; and

b) The PHI disclosed is limited to the following information:

- Name and address;
- Date and place of birth;
- Social security number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and

- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

As it relates to the Plan:

1. The Privacy & Security Officer will document any disclosures by whistleblowers and victims of crime, when it is brought to the Privacy & Security Officer's attention that such disclosures have been made.

2. The Privacy & Security Officer will ensure that such disclosures have been made to the appropriate parties as described in this Plan's Policy Statement above.

3. The Privacy & Security Officer will retain documentation related to such disclosures in accordance with the Plan's Record Retention policy.

4. Any disclosure for a victim of crime will be limited to the eight items described in the policy section above.

As it relates to Business Associates:

Business Associates shall implement procedures for disclosures of PHI by whistleblowers and victims of crime in compliance with Section 164.502(j) of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.502(j).
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy.

HIPAA POLICY AND PROCEDURE AND DOCUMENTATION OF HIPAA POLICIES AND PROCEDURES FOR COMPLIANCE WITH HIPAA RULES

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(i) and 164.316 of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

1. The Plan will implement policies and procedures with respect to PHI. The policies and procedures will be designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Rules.

2. The policies and procedures will be reasonably designed, taking into account the size of and the type of activities of this Plan that relate to PHI undertaken by the Plan, to ensure such compliance.

3. **Changes to policies or procedures**: The Plan will change its policies and procedures as necessary and appropriate to comply with changes in the law.

    a. When the Plan changes a privacy practice that is stated in the Plan's HIPAA Privacy Notice and makes corresponding changes to its policies and procedures, the Plan will make the changes effective for PHI that the Plan creates or receives prior to the effective date of the HIPAA Privacy Notice revision, if the Plan has included in the HIPAA Privacy Notice a statement reserving the Plan's right to make such a change in its privacy practices; or

    b. The Plan may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with the regulations (as outlined in the section of this policy regarding changes to policies or procedures that do NOT affect the HIPAA Privacy Notice).

4. **Changes in law:** Whenever there is a change in law that necessitates a change to the Plan's policies or procedures, the Plan will promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Plan's HIPAA Privacy Notice the Plan will promptly make the appropriate revisions to the Privacy Notice.

5. **Changes to privacy practices that are stated in the HIPAA Privacy Notice**: To implement a change the Plan will:

    a. Ensure that the policy or procedure, is revised to reflect a change in the Plan's privacy practice as stated in the Plan's Notice;

    b. Document the policy or procedure, as revised; and

    c. Revise the HIPAA Privacy Notice to state the changed practice and make the revised HIPAA Privacy Notice available as required by the regulations at § 164.520(c) See also the Plan's policy on Privacy Notices for information on the distribution of the Privacy Notice.

    d. The Plan will not implement a change to a policy or procedure prior to the effective date of the revised Privacy Notice.

e. If the Plan has not reserved its right to change a privacy practice as stated in the Plan's HIPAA Privacy Notice, the Plan will be bound by the privacy practices as stated in the Privacy Notice with respect to PHI created or received while such Privacy Notice is in effect. The Plan may change a privacy practice that is stated in the Privacy Notice, and the related policies and procedures, without having reserved the right to do so, provided that:

- Such change meets the implementation specifications 164.530(i)(4)(i)(A)-(C) of the regulations; and

- Such change is effective only with respect to PHI created or received after the effective date of the Privacy Notice.

6. **Changes to policies or procedures that do NOT affect the HIPAA Privacy Notice:** The Plan may change, at any time, a policy or procedure that does not materially affect the content of the Plan's HIPAA Privacy Notice provided that:

- The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of the regulations; and

- Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by the regulations.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

As it relates to the Plan:

1. The Privacy & Security Officer will retain documentation of the Plan's HIPAA policies and procedures and all changes in policies and procedures in accordance with the Plan's policy on Record Retention.

2. All policies and procedures are to be authorized by the Privacy & Security Officer.

3. The Privacy & Security Officer will review the HIPAA policies & procedures periodically and update as necessary.

4. The Privacy & Security Officer will promptly implement any necessary changes to policies or procedures.

5. If a change to a policy/procedure causes a material change to be made to the Plan's HIPAA Privacy Notice, Administrative Office staff on behalf of the Plan will follow the steps to be taken for a material change of a HIPAA Privacy Notice. See the Policy/procedure on Privacy Notice in this manual.

As it relates to Business Associates:

Business Associates shall implement written policies and procedures in compliance with Section 164.530(i) and 164.316 of the HIPAA Rules. Such procedures will be provided to the Plan upon request. The policies, procedures, and other documentation will be made available, as applicable to Business

Associates or other persons responsible for implementing the procedures to which the documentation pertains.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.530 and 164.316.
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy
- The Plan's Privacy Notice Policy

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.524 of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. **Individual's Access to PHI:** The Plan, through its Business Associates, will permit an individual to inspect and obtain a copy of PHI about the individual in a designated record set for as long as the PHI is maintained in the **designated record set,** except for:

   a. Psychotherapy notes,

   b. Information compiled in anticipation of, or for use in, a civil, criminal or administrative action or proceeding, or

   c. PHI maintained by the Plan that is subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or exempt from the Clinical Laboratory Improvements Amendments of 1988, 42 CFR 493.3(a)(2).

   The Business Associates, on behalf of the Plan will document the following and retain the documentation:

   - The designated record sets that are subject to access by individuals; and

   - The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

The Plan may require individuals to make requests for access in writing, provided that the Plan informs individuals of such a requirement. See also item 4 in this Policy for more information on timeliness.

The Plan must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about them in designated record sets. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the Plan need only produce the PHI once in response to a request for access.

If the Plan does not maintain the PHI that is the subject of the individual's request for access, and the Plan knows where the requested information is maintained, the Plan must inform the individual where to direct the request for access to PHI.

2. Plan's Denial of an Individual's Access to PHI: **The Plan may deny an individual access to PHI without providing the individual the opportunity for review, as follows**:

   a. If the information is excepted from the right of access by paragraph 1 a-c above; or

b. If the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;

c. An individual's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

The Plan must provide a timely, written denial to the individual, and the denial must be in plain language and contain:

- The basis for the denial;

- If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights; and

- A description of how the individual may complain to the Plan or to the Secretary of HHS. The description must include the name, or title, and telephone number of the Plan's Privacy & Security Officer.

3. **Individual's Right to Have a Denial of Access to PHI Reviewed:** The Plan may deny an individual access to PHI, provided that the individual is given a right to have such denial reviewed in the following circumstances:

   a. When 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;

   b. When 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; or

   c. When the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If access is denied on a ground permitted above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Plan to act as a reviewing Officer and who did not participate in the original decision to deny. The Plan must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination. The Plan must provide or deny access in accordance with the determination of the reviewing Officer.

4. **Timely Action by the Plan to a Request to Access PHI.** The Plan will act on a request for access no later than 30 days after receipt of the request as follows.

   a. If the Plan grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested.

b. If the Plan denies the request, in whole or in part, it must provide the individual with a written denial.

c. If the request for access is for PHI that is not maintained or accessible to the Plan on-site, the Plan must take an action by no later than 60 days from the receipt of such a request. If the Plan is unable to take an action required within the time required the Plan may extend the time for such action by no more than 30 days, provided that the Plan provides the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request. The Plan may have only one such extension of time for action on a request for access.

d. The Plan must arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mail the copy of the PHI at the individual's request. The Plan may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

e. If an individual's request for access directs the Plan to transmit the copy of PHI directly to another person designated by the individual, the Plan must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI.

5. **Plan's Obligation to Provide PHI in Form/Format Requested**: The Plan must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form or and format as agreed to by the Plan and the individual.

   If the PHI that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the Plan must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Plan and the individual.

   The Plan may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to such a summary or explanation and the individual agrees in advance to the fees imposed, if any, by the Plan for such summary or explanation.

6. **Fees:** If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, the Plan may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

   a. Copying, whether in paper or electronic, including the cost of supplies (for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media such as a CD or flash drive) and labor of copying (including time spent to create and copy the electronic file, such as compiling, extracting, scanning, and burning PHI to electronic media and distribution of the electronic media), the PHI requested by the individual;

   b. Postage, when the individual has requested the copy or electronic media, or the summary or explanation, be mailed; and

   c. Preparing an explanation or summary of the PHI, if agreed to by the individual.

d. The Plan may not charge retrieval fees (a standard retrieval fee, a fee for the actual cost of retrieval), or fees associated with maintaining systems and recouping capital for data access, storage and infrastructure.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Designated record set** means, at a minimum, the records maintained by or for the Plan relating to the covered individual's enrollment, payment, claims adjudication, case or medical management record systems that are used in whole or in part by the Plan to make decisions about individuals. Records that otherwise meet the definition of designated record set and which are held by a Business Associate, when acting on behalf of the Plan, are part of the Plan's designated record set.

  Designated Record set does not include, psychotherapy notes, claim audit files, records prepared for litigation, health information that is not used to make decisions about individuals or information that the individual does not have a right to access based on state or Federal law, quality and operational improvement records, risk management records. The Privacy & Security Officer (or designee) is responsible for determining what constitutes the designated record set of this Plan.

- **Record** means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Plan. The record may contain electronic and paper documents.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates are required to implement procedures to comply with the HIPAA Privacy requirements on behalf of the Plan and shall implement procedures to allow individuals access to their PHI in compliance with Section 164.524 of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.524

- The Plan's Privacy & Security Officer

HIPAA POLICY AND PROCEDURE ON RIGHT TO REQUEST PRIVACY PROTECTION (RESTRICTIONS) ON USE AND DISCLOSURE OF PHI

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.522 of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan, through its Business Associates, will permit an individual to request, in writing, that the Plan **restrict the use and disclosure** of that individual's PHI:

- To carry out treatment, payment and health care operations (TPO)
- To persons involved in an individual's care and
- For notification purposes.

The Plan, however, is **not required to agree to the request to restrict PHI** if the Business Associate determines the request to be unreasonable, e.g.*, if it would interfere with the Plan's ability to pay a claim.*

EXCEPTION IN EMERGENCY: If the Plan agrees to the requested restriction, it will not violate the restriction except if the individual is in need of emergency treatment, and the restricted PHI is needed to provide the emergency treatment.

- The Plan may use the restricted PHI, and may disclose this information to a health care provider in order to provide the needed treatment to the individual.
- If restricted PHI is disclosed to a health care provider because it is necessary for emergency treatment, the Plan will request that the health care provider not further use or disclose the information.
- The Plan must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if:
  - The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
  - The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the Covered Entity in full.

The Plan's agreement to a restriction on the use or disclosure of PHI is not effective to prevent the following uses or disclosures:

1. When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with HIPAA, or
2. For instances where an authorization is not required under the Plan's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.

The Plan's agreement to a restriction is binding only on the Plan and its Business Associates, not on other entities such as insurers or health care providers.

Separately, the Plan acknowledges and understands that **individuals have the right to request that PHI related to services or items for which they have paid out-of-pocket in full, not be disclosed to the Plan**, and that such requests must be granted if the disclosure would be for payment or health care operations purposes and the disclosure is not otherwise required by law. These requests will generally be directed to health care providers, but may result in PHI not being shared with the Plan.

The Plan will notify its pertinent Business Associates of the existence of a notice of restriction.

The Plan must document a restriction and keep the documentation in accordance with record keeping requirements of the Plan.

The Plan may terminate the agreement to restrict PHI only if the following occurs:

1. The individual agrees to or requests the termination in writing;

2. The individual verbally agrees to the termination and the oral agreement is documented; or

3. The Covered Entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates required to implement procedures to comply with the HIPAA Privacy requirements on behalf of the Plan, shall implement procedures to allow individuals to request restriction of uses and disclosures to their PHI in compliance with Section 164.522 of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.522.

- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE FOR REQUESTING THAT PHI BE TRANSMITTED CONFIDENTIALLY (e.g. by Alternate Means or Location)

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.522(b) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

The Plan, through its Business Associates, will permit and accommodate an individual's reasonable written request to have PHI sent by alternative means or to an alternative location, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

The Plan will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates required to implement procedures to comply with the HIPAA Privacy requirements on behalf of the Plan, shall implement procedures to allow individuals to request restriction of the uses and disclosures of their PHI in compliance with Section 164.522(b) of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.522(b).
- The Plan's Privacy & Security Officer.

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.526 of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. **Right to amend:** An individual has the right to have the Plan amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

2. **Denial of amendment:** The Plan, through its Business Associates, may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:

   a. Was not created by the Plan, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;

   b. Is not part of the designated record set;

   c. Would not be available for inspection under the "Access to PHI" policy; or

   d. Is accurate and complete.

3. **Individual's request for amendment:** The Plan must permit an individual to request that the Plan amend the PHI maintained in the designated record set. The Plan may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. The right to amend PHI applies only for as long as the PHI is maintained in a designated record set.

4. **Timely action by the Plan:** The Plan must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

   a. If the Plan grants the requested amendment, in whole or in part, it must take the actions required by paragraphs 5a and b below.

   b. If the Plan denies the requested amendment, in whole or in part, it must provide the individual with a timely written denial as outlined in this policy.

   If the Plan is unable to act on the amendment within the time required by this policy, the Plan may extend the time for such action by no more than 30 days, provided that:

   a. The Plan, no later than 60 days after receipt of such a request, provides the individual with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request; and

   b. The Plan may have **only one such extension** of time for action on a request for an amendment.

5. **Accepting the amendment:** If the Plan accepts the requested amendment, in whole or in part, the Plan must comply with the following requirements.

a. **Making the Amendment**: The Plan must make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. The right to amend does not include the right for a covered individual to make the actual changes to PHI.

b. **Informing the Individual**: The Plan must timely inform the individual that the amendment is accepted and obtain the individual's identification of, and agreement to have the Plan notify the relevant persons with which the amendment needs to be shared in accordance with the following paragraph 5c.

c. **Informing Others**: The Plan must make reasonable efforts to inform and provide the amendment within a reasonable time to:

- Persons identified by the individual as having received PHI about the individual and needing the amendment; and

- Persons, including Business Associates, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

6. **Denying the amendment:** If the Plan denies the requested amendment, in whole or in part, the Plan must comply with the following requirements.

a. Provide the individual with a timely, written denial, in accordance with this policy. The **denial must use plain language and contain**:

- The basis for the denial, (see paragraph 2 above);

- The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

- A statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

- A description of how the individual may complain to the Plan or to the HHS Secretary. The description must include the name, or title, and telephone number of the Privacy & Security Officer.

7. **Statement of disagreement**: The Plan must permit the individual to submit to the Plan a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The Plan may reasonably limit the length of a statement of disagreement. The Plan may prepare a written **rebuttal** to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the Plan must provide a copy to the individual who submitted the statement of disagreement.

8. **Recordkeeping**: The Plan must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any, to the designated record set.

9. **Future disclosures**: If a statement of disagreement has been submitted by the individual, the Plan must include the material appended in accordance with paragraph 7 above, or, at the election of the Plan, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.

   If the individual has not submitted a written statement of disagreement, the Plan must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action in accordance with paragraph 6a above.

   When a subsequent disclosure is made using a standard HIPAA Electronic Data Interchange (EDI) transaction that does not permit the additional material to be included with the disclosure, the Plan may separately transmit the material, as applicable, to the recipient of the standard transaction.

10. **Actions on notices of amendment**: If the Plan is informed by another Covered Entity (e.g. group health plan, health care provider or clearinghouse) of an amendment to an individual's PHI, in accordance with paragraph 5c above, the Plan must amend the PHI in designated record sets as provided by paragraph 5a above.

11. **Documentation**: The Plan must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by the regulations (see this Plan's policy on Record Retention).

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Designated record set means**, at a minimum, the records maintained by or for the Plan relating to the covered individual's enrollment, payment, claims adjudication, case or medical management record systems that are used in whole or in part by the Plan to make decisions about individuals. Records that otherwise meet the definition of designated record set and which are held by a Business Associate, when acting on behalf of the Plan, are part of the Plan's designated record set.

  Designated Record set does not include, psychotherapy notes, claim audit files, records prepared for litigation, health information that is not used to make decisions about individuals or information that the individual does not have a right to access based on state or Federal law, quality and operational improvement records, risk management records. The Privacy & Security Officer (or designee) is responsible for determining what constitutes the designated record set of this Plan.

- **Record means** any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the Plan. The record may contain electronic and paper documents.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates required to implement procedures to comply with the HIPAA Privacy requirements on behalf of the Plan, shall implement procedures to allow individuals to request to amend their PHI in compliance with Section 164.526 of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.526
- The Plan's Privacy & Security Officer
- The Plan's Record Retention Policy

HIPAA POLICY AND PROCEDURE ON THE RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.528 of the HIPAA Rules under the health insurance portability and accountability act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), we will follow the revised rules.

1. **Individual Rights:** An individual has **a right to receive an accounting of disclosures of PHI made by the Plan in the six years prior** to the date on which the accounting is requested in writing, **except for** disclosures:

    a. To carry out treatment, payment and health care operations;

    b. To individuals referencing the PHI about themselves;

    c. Incident to a use or disclosure otherwise permitted or required by the privacy regulation;

    d. Pursuant to an authorization;

    e. For the facility's directory or to persons involved in the individual's care or other notification purposes (§ 164.510);

    f. For national security or intelligence purposes as provided in Section 164.512(k)(2);

    g. To correctional institutions or law enforcement officials as provided in Section 164.512(k)(5);

    h. As part of a limited data set in accordance with Section 164.514(e); or

    i. That occurred prior to the compliance date for the Plan.

2. **Suspension of Rights:** The Plan must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, (as provided in § 164.512(d) or (f), respectively), for the time specified by such agency or official, if such agency or official provides the Plan with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made **verbally**, the Plan must:

    a. Document the statement, including the identity of the agency or official making the statement;

    b. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

    c. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

    An individual may request an accounting of disclosures for a period of time **less than** six years from the date of the request.

3. **Content of the accounting.** The Plan must provide the individual with a written accounting that meets the following requirements.

   a. The accounting must include disclosures of PHI that occurred during the six years (or such shorter time period at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by Business Associates of the Plan.

   b. The **accounting must include** for each disclosure:

      i. The date of the disclosure;

      ii. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

      iii. A brief description of the PHI disclosed; and

      iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement, a copy of a written request for a disclosure, if any, (see also Sections 164.502(a)(2)(ii) or 164.512,).

   c. If, during the period covered by the accounting, the Plan has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:

      i. The information required for the first disclosure during the accounting period;

      ii. The frequency, periodicity, or number of the disclosures made during the accounting period; and

      iii. The date of the last such disclosure during the accounting period.

      iv. If, during the period covered by the accounting, the Plan has made disclosures of PHI for a particular research purpose for 50 or more individuals (in accordance with §164.512(i)), the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

         A. The name of the protocol or other research activity;

         B. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

         C. A brief description of the type of PHI that was disclosed;

         D. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

         E. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

         F. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If the Plan provides an accounting for research disclosures, (in accordance with 164.528(b)(4)), and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the Plan will, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

4. **Provision of the accounting:** The Plan must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

   a. The Plan must provide the individual with the accounting requested; or

   b. If the Plan is unable to provide the accounting within the time required, the Plan may extend the time to provide the accounting by no more than 30 days, provided that:

      - The Plan, within 60 days after receipt of such a request, provides the individual with a written statement of the reasons for the delay and the date by which the Plan will provide the accounting; and

      - The Plan may have only one such extension of time for action on a request for an accounting.

   c. The Plan will provide the first accounting to an individual in any 12-month period without charge.

   d. The Plan may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the Plan informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

5. **Documentation:** The Plan must document the following and retain the documentation for six years:

   a. The information required to be included in an accounting for disclosures of PHI that are subject to an accounting;

   b. The written accounting that is provided to the individual under this section; and

   c. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Reasonable, cost-based fee** means postage, supplies, labor related to copying. It does not mean cost/labor associated with searching for and retrieving the requested information.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Those Business Associates required to implement procedures to comply with the HIPAA Privacy requirements on behalf of the Plan, shall implement procedures to allow individuals to request an accounting of uses and disclosures of their PHI in compliance with Section 164.528 of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR 164.528
- The Plan's Privacy & Security Officer

HIPAA POLICY AND PROCEDURE FOR WAIVER OF RIGHTS

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(h) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

The Plan **may not** require individuals to waive their rights to file a complaint with the Secretary (Section 164.306) or any other rights guaranteed under the HIPAA Privacy regulations as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Business Associates shall implement procedures to not require individuals to waive certain rights, in compliance with Section 164.530(h) of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.530(h).
- The Plan's Privacy & Security Officer.

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514(e) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

1. **Limited data set:** The Plan, through its Business Associates, may use or disclose a limited data set of PHI that meets the definition of limited data set along with the requirements of paragraph 2 below, if the Plan enters into a data use agreement with the limited data set recipient, in accordance with paragraph 3 of this policy.

2. **Permitted purposes for uses and disclosures:** The Plan may use or disclose a limited data set (as defined in these policies and procedures) only for the purposes of research, public health, or health care operations. The Plan may use PHI to create a limited data set that meets the definition of limited data set, or the Plan may disclose PHI to a Business Associate for the purpose of using PHI to create a limited data set, whether or not the limited data set is to be used by the Plan.

3. **Data Use Agreement:** The Plan may use or disclose a limited data set under paragraph 1 of this policy only if the Plan obtains satisfactory assurance, in the form of a "data use agreement" that meets the requirements of this policy, that the limited data set recipient will only use or disclose the PHI for limited purposes.

   Contents of a Data Use Agreement. A data use agreement between the Plan and the limited data set recipient must:

   a. Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph 2 of this policy. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the Plan.

   b. Establish who is permitted to use or receive the limited data set; and provide that the limited data set recipient will:

      1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

      2) Use appropriate safeguards to prevent use or disclosure of the information, including electronic PHI, other than as provided for by the data use agreement;

      3) Report to the Plan any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

      4) Ensure that any agents, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information;

      5) Not identify the information or contact the individuals

4. **Compliance:** The Plan is not in compliance with the standards of this policy if the Plan knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the Plan took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

   a. Discontinued disclosure of PHI to the recipient; and

   b. Reported the problem to the Secretary of HHS.

   If this Plan received a limited data set and violates a data use agreement this Plan will be in noncompliance with the standards, implementation specifications, and requirements of this policy.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **Limited data set means** PHI that **excludes** the following direct identifiers of the individual or of relatives, employers, or household members of the individual
  - Names;
  - Postal address information, other than town or city, State, and zip code;
  - Telephone numbers and Fax numbers;
  - Electronic mail addresses;
  - Social security numbers;
  - Medical record numbers
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/license numbers;
  - Vehicle identifiers and serial numbers, including license plate numbers;
  - Device identifiers and serial numbers;
  - Web Universal Resource Locators (URLs);
  - Internet Protocol (IP) address numbers;
  - Biometric identifiers, including finger and voice prints; and
  - Full face photographic images and any comparable images.

The following direct identifiers **are not part of a limited data set**:

- admission,
- discharge and service dates,
- date of death,
- age and
- five digit zip code (**for public health, research or health care operations*). *See: http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm#box3

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for processing this policy to contracted Business Associates. Business Associates shall implement procedures for limited data set in compliance with Section 164.514(e) of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.514(e).
- The Plan's Privacy & Security Officer.

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514(f) and (g) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

1. **Uses and disclosures of PHI for Fundraising.** The Plan may use, or disclose to a Business Associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without a valid authorization:

   a. Demographic information relating to an individual, including name, address, other contact information, age, gender and date of birth; and

   b. Dates of health care provided to an individual;

   c. Department or service information;

   d. Treating physician;

   e. Outcome information and;

   f. Health insurance status.

   The Plan may not use or disclose PHI for fundraising purposes as otherwise permitted by paragraph 1 of this policy unless a statement is included in the Plan's HIPAA Privacy Notice (as required by § 164.520(b)(1)(iii)(B)).

   The Plan must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

   - The Plan may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

   - The Plan may not make fundraising communications to an individual where the individual has elected not to receive such communications.

   - The Plan may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

2. **Uses and disclosures of PHI for Underwriting and related purposes**:

If a health plan receives PHI for the purpose of underwriting, enrollment, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such PHI for such purpose as may be required by law, subject to the

prohibition with respect to genetic information included in the PHI. See also the policy/procedure in this manual related to Limitations on the Use and Disclosure of Genetic Information.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, does not use or disclose PHI for fundraising purposes. Business Associates are required to limit fundraising communications to individuals in compliance with Section 164.514(f) of the HIPAA Rules.

The Plan Sponsor, on behalf of the Plan, may request Business Associates to disclose PHI (excluding genetic information) for the purpose of underwriting, enrollment, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits. The recipient of the PHI will be required to only use the PHI for the purpose intended and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such PHI for such purpose as may be required by law, subject to the prohibition with respect to genetic information included in the PHI.

Each Business Associate will retain documentation in accordance with the Plan's Record Retention Policy.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions and Limitations on the Use and Disclosure of Genetic Information.

ADDITIONAL RESOURCES

- 45 CFR, Section 164. 514(f) and (g).
- The Plan's Privacy & Security Officer.
- The Plan's policy on Authorizations.
- The Plan's Record Retention Policy

HIPAA POLICY AND PROCEDURE FOR MARKETING AND PROHIBITION ON SALE OF PHI

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.501, 164.508(a)(3) and (a)(4), and 164.502(a)(5)(ii) of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

Marketing

Section 164.508 (a) addresses that an **Authorization is required for marketing**. The authorization must state the Plan will receive financial remuneration from or on behalf of the third party whose items or services are being marketed, and must be signed and received by the Plan before the marketing activity begins:

Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, the Plan must obtain an authorization for any use or disclosure of PHI for marketing.

If the marketing involves direct or indirect financial remuneration (defined in this policy under Key Definitions) to the Plan from a third party, the authorization must state such remuneration is involved.

Prohibition on Sale of PHI Policy

Subject to the exceptions below, the Plan will obtain an authorization to disclose PHI if it is receiving direct or indirect remuneration from or on behalf of the recipient of the information in exchange for the information. (The authorization must state the Plan will receive remuneration in the form of payment or other benefit for disclosing or selling the PHI, and must be signed and received by the Plan before the marketing activity begins.) For this purpose, "sale of PHI" includes transactions that involve a transfer of ownership of PHI, as well as exchanges of PHI under access, license or lease agreements, and any other exchanges of PHI for which remuneration is made.

- **Remuneration includes** financial payments or non-financial benefits (such as benefits in-kind).
- **Direct remuneration** is that which is received directly from the recipient of the PHI and **indirect remuneration** is that which is received on behalf of the recipient of the PHI from another entity.

The following disclosures are excepted from the prohibition on the sale of PHI and therefore, **no authorization is required to make these disclosures** under 164.512(b) or 164.514(e):

- Disclosures for public health purposes under 164.512(b) or 164.514(e);
- For research purposes pursuant to 164.512(i) or 164.514(e) as long as remuneration is subject to certain limitations;
- For treatment and payment purposes;

- For the sale transfer, merger or consolidation of all or part of the Plan and for related due diligence;

- To a Business Associate for activities that the Business Associate undertakes on behalf of the Plan, and the only remuneration is for the performance of the Business Associate activities on behalf of the Plan;

- To an individual who makes a request for access (See the Policy on Right of Access to PHI) or a request for an account of disclosure (see the Policy on Right of Accounting of Disclosures of PHI);

- As required by law as permitted under 164.512(a);

- For any other purpose permitted by these policies and procedures and the privacy rule, as long as any remuneration is limited to a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for that purpose, or a fee that is permissible by other law.

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

As defined in Section 164.501, **Marketing means (and an authorization will be obtained)**:

1. To make a communication (from the Plan or its Business Associate) about a product or service that encourages recipients of the communication to purchase or use the product or service, and for which, in exchange for making the communication, the Plan (or its Business Associate) receives direct or indirect financial remuneration from the entity whose product or service is being marketed.

   i. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

   ii. For treatment of the individual; or

   iii. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

2. For marketing purposes, **financial remuneration means** direct payment from the third party whose product or service is being described in the marketing communication, or indirect payment from another entity on behalf of the third party whose product or service is being described in the marketing communication. **Financial remuneration does not include** non-financial benefits such as in-kind benefits, or financial payments made for purposes other than marketing.

   Direct or indirect payment does not include any payment for treatment of an individual.

3. The following activities are not marketing and therefore can be done without the Plan obtaining an individual's authorization. **Marketing does not include** a communication made:

   i. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Covered

Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication. In addition to refill reminders, these communications may include information about generic equivalents, medication adherence or how to take biologic or self-administered medication. **If the financial remuneration received by the Plan is in excess of the costs reasonably related to making the communication, the communication will be a marketing communication for which authorization is required.**

ii. For the following treatment and health care operations purposes, except where the Covered Entity receives financial remuneration in exchange for making the communication:

A. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

B. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

C. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

The following communications are not marketing communications for which an authorization is required even if financial remuneration is received:

- A face to face communications by the entity (the Plan) with the individual whose PHI is being disclosed; or

- A promotional gift of nominal value to the individual whose PHI is being disclosed.

- Communications promoting a healthy diet or encouraging individuals to get certain routine diagnostic tests do not constitute marketing and do not require an authorization.

PROCEDURES

The Plan does not sell or market PHI to a Business Associate or any other third party for that party's own purposes. The Plan will not sell or market lists of Individuals or enrollees to third parties without obtaining authorization from each person on the list. Should the Plan consider an opportunity to sell or market PHI it shall consult with legal counsel.

Business Associates shall implement procedures for marketing and sale of PHI in compliance with Section 164.501, 164.508(a)(3) and (a)(4), and 164.502(a)(5)(ii) of the HIPAA Rules. Such procedures will be provided to the Plan upon request.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164. 501 and 164.508(a)(3) and (a)(4), 164.502(a)(5)(ii).
- The Plan's Privacy & Security Officer.
- Refer to the policy on Authorizations.

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 160.203-205 of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

This Plan recognizes that certain state laws may be more stringent than the Federal HIPAA Privacy regulation requirements. The Plan will adhere to state laws that are more stringent than the Federal law, where applicable to the Plan.

Preemption of State Law - General Rule and Exception - § 160.203

A standard, requirement, or implementation specification adopted under the HIPAA Privacy regulations that is **contrary** to a provision of State law preempts the provision of State law. When used to compare a provision of State law to a HIPAA Privacy standard, requirement or implementation specification, **contrary means** that the Plan would find it impossible to comply with both the State and Federal requirements or the state law stands as an obstacle to accomplishing the full purpose and objectives of the Federal law.

This general rule applies, except if one or more of the following conditions is met:

a. A determination is made by the Secretary of the Department of Health and Human Services (HHS) that the provision of State law is necessary:

- To prevent fraud and abuse related to the provision of or payment for health care;
- To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
- For State reporting on health care delivery or costs; or
- For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under the HIPAA Rules is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

    a. Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

    b. The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under the HIPAA Privacy regulations.

    c. The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

d. The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

Process for Requesting Exception Determinations - § 160.204

A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary of HHS. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

1. The State law for which the exception is requested;

2. The particular standard, requirement, or implementation specification for which the exception is requested;

3. The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

4. How health care providers, health plans, and other entities would be affected by the exception;

5. The reasons why the State law should not be preempted by the Federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

6. Any other information the Secretary may request in order to make the determination.

Requests for exception must be submitted to the Secretary of HHS. Until the Secretary's determination is made, the standard, requirement, or implementation specification under the HIPAA Privacy regulations remains in effect. The Secretary's determination will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

Duration of Effectiveness of Exception Determinations - § 160.205

An exception granted under the HIPAA Privacy regulation remains in effect until:

a. Either the State law or the Federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

b. The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

KEY DEFINITIONS

In addition to the terms defined on the cover page of this manual, the following term(s) found in this Policy and Procedure mean:

- **State law** means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

- **State** refers to one of the following:

1. For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

2. For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

- **Relates to the privacy of individually identifiable health information** means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

- **More stringent** means, in the context of a comparison of a provision of State law and a standard, requirement or implementation specification adopted under Subpart E of Section 164 of the HIPAA Rules, a State law meets one or more of the following criteria:

  1. With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

     - Required by the Secretary in connection with determining whether a Covered Entity or Business Associate is in compliance with the HIPAA Rules; or

     - To the individual who is the subject of the individually identifiable health information.

  2. With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

  3. With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

  4. With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

  5. With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

  6. With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

- **Contrary**, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

  1. A Covered Entity or Business Associate would find it impossible to comply with both the State and Federal requirements; or

2. The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, Section 264 of Public Law 104-191, or Sections 13400-13424 of Public Law 111-5, as applicable.

PROCEDURES

If any state laws affect these policies and procedures, the Privacy & Security Officer will work with legal counsel to include reference to any such laws in this section.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 160.203-205.
- The Plan's Privacy & Security Officer.

HIPAA POLICY AND PROCEDURE ON NOTIFICATION IN THE CASE OF A BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (PHI)

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, and 164.414 of the HIPAA Rules under the Federal regulation, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) and their implementing regulations and guidance. If the HIPAA Rules are changed by the Department of Health and Human Services (HHS), this Plan will follow the revised rules.

Effective Date: The requirements of this policy shall apply with respect to breaches of PHI occurring **on or after September 23, 2009, as amended September 23, 2013**.

§ 164.404 Notification to Individuals.

1. **Standard-General rule**. A Covered Entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

2. **Breaches treated as discovered**. A breach shall be treated as discovered by a Covered Entity as of the first day on which such breach is known to the Covered Entity, or, by exercising reasonable diligence would have been known to the Covered Entity.

3. A Covered Entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Covered Entity (determined in accordance with the Federal common law of agency).

4. **Implementation specification: Timeliness of notification**. Except as provided in § 164.412, a Covered Entity shall provide the notification required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

5. **Implementation specifications: Content of notification.**

    a. **Elements**. The notification required shall include, to the extent possible:

        i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

        ii. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

        iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

        iv. A brief description of what the Covered Entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

v. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

b. **Plain language requirement**. The notification required shall be written in plain language.

6. **Implementation specifications: Methods of individual notification.** The notification required shall be provided in the following form:

   a. **Written notice.**

      i. Written notification by **first-class mail** to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

      ii. If the Covered Entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

7. **Substitute notice.** In the case in which there is **insufficient or out-of-date contact information** that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.

   a. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

   b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

      i) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the Covered Entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

      ii) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

8. **Additional notice in urgent situations.** In any case deemed by the Covered Entity to require urgency because of possible imminent misuse of unsecured PHI, the Covered Entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice.

§ 164.406 Notification to the Media.

1. **Standard.** For a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, a Covered Entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.

2. **Implementation specification: Timeliness of notification.** Except as provided in § 164.412, a Covered Entity shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

3. **Implementation specifications: Content of notification**. The notification required shall meet the requirements of § 164.404.

§ 164.408 Notification to the Secretary.

1. Standard. A Covered Entity shall, following the discovery of a breach of unsecured PHI as provided in § 164.404, **notify the Secretary**.

2. **Implementation specifications: Breaches involving 500 or more individuals**. For breaches of unsecured PHI involving 500 or more individuals, a Covered Entity shall, except as provided in § 164.412, provide the notification required contemporaneously with the notice required by §164.404 and in the manner specified on the HHS web site.

3. **Implementation specifications: Breaches involving less than 500 individuals**. For breaches of unsecured PHI involving less than 500 individuals, a Covered Entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for breaches occurring during the preceding calendar year, in the manner specified on the HHS web site.

§ 164.410 Notification by a Business Associate.

1. **Standard.** A Business Associate shall, following the discovery of a breach of unsecured PHI, notify the Covered Entity of such breach.

2. **Breaches treated as discovered.** For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a Business Associate as of the first day on which such breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the Business Associate (determined in accordance with the Federal common law of agency).

3. **Implementation specifications: Timeliness of notification**. Except as provided in § 164.412, a Business Associate shall provide the notification required without unreasonable delay and **in no case later than 60 calendar days** after discovery of a breach. Plans may negotiate a tighter notification deadline, such as 30 days or 45 days with a Business Associate.

4. **Implementation specifications: Content of notification**.

    a. The notification required shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the breach.

    b. A Business Associate shall provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual at the time of the notification required or promptly thereafter as information becomes available.

§ 164.412 Law Enforcement Delay.

1. **If a law enforcement official states** to a Covered Entity or Business Associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a Covered Entity or Business Associate shall:

   a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

   b. If the statement is made verbally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

§ 164.414 Administrative Requirements and Burden of Proof.

1. **Administrative requirements.** A Covered Entity is required to comply with the administrative requirements of §§ 164.530(b) (*train workforce*), (d) (*provide a process for individuals to complain*), (e) (*have and apply appropriate sanctions*), (g) (*refrain from intimidating or retaliatory acts*), (h) (*may not require individuals to waive their rights*), (i) (*must implement policies and procedures to comply with standards*), and (j) (*change policies and procedures as necessary*) with respect to the requirements of this subpart.

   Burden of proof. In the event of a use or disclosure in violation, the Covered Entity or Business Associate, as applicable, shall have the burden of demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach, as defined at § 164.402 (*see Key Definitions below*).

KEY DEFINITIONS

For assistance understanding common terms used in this manual, refer to the cover page.

§ 164.402 Definitions.

Breach means the acquisition, access, use, or disclosure of (unsecured) PHI in a manner not permitted under subpart E of the HIPAA Rules which compromises the security or privacy of the PHI. *(Note: The HIPAA Rules is contained in Subpart E. Subpart E extends from §164.500 through §164.534.)*

- For an incident or breach investigation prior to September 23, 2013, for purposes of this definition, **compromises the security or privacy of the PHI** means poses a **significant risk of financial, reputational, or other harm to the individual**. See below for an incident or breach investigation on or after September 23, 2013.

- A use or disclosure of PHI that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes:

- **Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a Covered Entity or a Business Associate**, if such acquisition, access, or

use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under Subpart E of the HIPAA Rules.

- **Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate,** or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under Subpart E of the HIPAA Rules.

- **A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief** that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

For an incident or breach investigation **on or after September 23, 2013**:

If a violation does not fit into one of the three exclusions noted above, the Privacy & Security Officer **will presume that a breach of unsecured PHI has occurred** unless a risk assessment, conducted in accordance with these procedures, determines that there is a **low probability** that the PHI has been compromised. If the Privacy & Security Officer determines there has been a breach of unsecured PHI, the Plan will provide notification in accordance with these procedures.

Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS (in the guidance issued under Section 13402(h)(2) of Pub. L. 111-5 on the HHS web site). At this time, the HHS-specified technologies and methodologies to **secure PHI** are:

a. **Encryption for electronic PHI** "in motion," "at rest," and "in use." The Plan's encryption policies, if any, are described in its HIPAA Security Policies and Procedures.

b. **Destruction by shredding** for hardcopy PHI, whether documents, discs, tapes, flash drives or any other portable technology. Electronic PHI is destroyed in accordance with the applicable guidance issues by HHS. The Plan's Security Policies/procedures describe its procedures for the destruction of electronic PHI, if any.

Health information means any information, including genetic information, whether oral or recorded in any form or medium that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. Relates to the 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.

PROCEDURES

1. The Plan requires all Business Associates, Workforce Members and Plan Sponsor to report (to the Plan's Privacy & Security Officer) any use or disclosure of PHI that might be a violation of the Plan's HIPAA policies and procedures.

Reports may be made verbally or in writing, but must be provided immediately upon committing any action that the person believes may have violated the Plan's HIPAA policies and procedures or immediately upon learning that another member of the workforce or any other person (such as a Business Associate) may have done something that may be in violation of the Plan's HIPAA policies and procedures.

2. The Privacy & Security Officer will:

   a) Accept reports from any person who believes there may have been a violation of the Plan's HIPAA policies and procedures. If the incident or breach occurred by a Business Associate or its agents/subcontractors, the Privacy & Security Officer will obtain a copy of the most current Business Associate Agreement with the Plan to review if there are unique provisions about how an incident or breach is to be managed that will need to be considered in addition to Federal law requirements and the process outlined in these procedures. For instance, sometimes the Business Associate Agreement requires the Business Associate to report an incident or breach to the Plan in less than the legally allowed 60 day period.

   b) Investigate the alleged violation of the Plan's HIPAA policies and procedures, (including reviewing the "policy statement" section at the beginning of this document).

   c) Question the person or workforce member reporting the perceived violation,

   d) Question the workforce member or other person who is alleged to have violated the Plan's HIPAA policies and procedures,

   e) Question other persons or workforce members who may have information about the alleged violation,

   f) Determine, in consultation with other workforce members (and the Plan's professional advisors, as appropriate), whether there has been a breach of unsecured PHI, as defined in the Plan's Breach Notification Policy Statement and in the regulations, Section 164.402 (meaning there has been an acquisition, access, use or disclosure of PHI not permitted by the privacy rule that has compromised the security or privacy of the PHI).

   g) Make and keep a written record of the HIPAA incident investigation and of the determination whether there <u>has or has not</u> been a breach of unsecured PHI.

3. If the Privacy & Security Officer may have been responsible (or partly responsible) for an incident that may be or is a breach of unsecured PHI, the incident will be investigated by an alternate designee, and this designee will work with legal counsel to make the determination whether there has been a breach requiring notification.

4. Legal counsel may need to be contacted to assist with determining if the incident is truly a breach.

5. The Privacy & Security Office will save the documentation of this research and risk assessment process regardless of whether the outcome of the research shows that the incident is or is not a breach.

6. The Privacy & Security Officer will complete the Plan's HIPAA Incident Log in order to track both non-breach incidents and true breach situations.

Notification to an Individual of a Breach of Unsecured PHI

1. The Privacy & Security Officer will, following the discovery of a breach of unsecured PHI, determine the responsibility of issuance of the notification to individuals and ensure that the responsible entity notify each individual whose unsecured PHI has been – or is reasonably believed to have been – accessed, acquired, used or disclosed as a result of the breach.

2. The Privacy & Security Officer will ensure that the responsible entity, as set forth in the Business Associate Agreement, provide the notice to each individual without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

    a. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. See the Law Enforcement Delay section below.

3. The individual notices will be in writing, in plain language, and will include, to the extent possible, all of the following points:

    a. A brief description of what happened (including the date of the breach and the date of the discovery of the breach, if known),

    b. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved) – without listing the actual individual identifiers or other sensitive information involved,

    c. Any steps that individuals should take to protect themselves from potential harm resulting from the breach,

    d. A brief description of what the Plan is doing to (i) investigate the breach, (ii) mitigate harm to the individual, and (iii) protect against further breaches, and

    e. Contact information for individuals to ask questions or learn information, including a toll-free phone number, an email address, a Web site, or postal address.

4. The Privacy & Security Officer will ensure that the responsible entity mails these notices, by first-class mail, to the individual's last known address. The notification may be provided in one or more mailings as information is available.

    a. Or, if the individual agrees to electronic notice and such agreement has not been withdrawn, the responsible entity will provide the notice by electronic mail.

    b. If the responsible entity knows the individual is deceased and has the address of next of kin or personal representative, the notice will be mailed to that person.

    c. If the individual affected by breach is a minor or otherwise lacks legal capacity due to a physical or medical condition, the responsible entity will provide the notice to the individual's personal representative (who, in the case of a minor child, will typically be the child's parent).

    d. If the responsible entity has insufficient or out-of-date contact information for fewer than 10 individuals, it will use an alternate form of notice such as telephone.

e. If the responsible entity has insufficient or out-of-date contact information for 10 or more individuals, it will notify those individuals either through a conspicuous posting on the Plan's Web site for a period of 90 days or in appropriate major print or broadcast media.

f. **Urgent Situation**: In situations deemed urgent by the responsible entity due to the possible imminent misuse of unsecured PHI, the responsible entity may provide notice to the affected individual(s) by phone or other means, in addition to providing the individual written notice.

Notification to the Secretary of Health and Human Services (HHS)

1. For breaches of unsecured PHI that involve fewer than 500 individuals, the responsible entity will keep a log and report these breaches to HHS on an annual basis. The reporting of breaches to HHS will occur not later than 60 days after the end of each calendar year in which the breach was discovered by the responsible entity, and will be performed in the manner specified on the HHS Web site. The Plan may opt to report breaches to HHS at the same time it sends notices to individuals, in the manner specified on the HHS web site.

2. For breaches of unsecured PHI involving 500 or more individuals, the responsible entity will notify HHS at the same time it provides the individual notices required above, and the reporting will be performed in the manner specified on the HHS Web site.

3. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. See the Law Enforcement Delay section below.

4. HHS Website is located at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Notification to the Media For Breaches Involving 500+ Individuals

1. For breaches involving more than 500 residents of one state or one jurisdiction (*i.e.*, a geographic area smaller than a state, such as a county, city or town), the responsible entity will notify prominent media outlets serving the state or jurisdiction at the same time it provides the individual notices required above. The notification to media outlets will be in the form of a press release.

2. The responsible entity will provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The responsible entity must notify the media directly and not by posting the notification on its website. It is not required to incur any cost to print or run a media notice.

3. Notification may be delayed at the request of a law enforcement official if the official states that notice would impede a criminal investigation or cause damage to national security. See the Law Enforcement Delay section below.

Breach by Business Associate (BA) or Subcontractor of a Business Associate

1. Through its Business Associate Agreements or otherwise, the Business Associates will require its subcontractors to promptly notify the Privacy & Security Officer of the Plan of any breach of unsecured PHI for which the Business Associate or one of its agents/subcontractors is or may be responsible. The notice will occur without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

2. Through its Business Associate Agreement or otherwise, the Business Associates will determine whether any required notices will be provided by the Privacy & Security Officer or by the applicable Business Associate.

    a. The Business Associate notification required will include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the breach.

    b. The Business Associate will provide the Plan with any other available information that the Plan is required to include in notification to the individual at the time of the notification required or promptly thereafter as information becomes available.

Law Enforcement Delay

1. If a law enforcement official states to the Privacy & Security Officer, or the Plan's Business Associate, that a notification, notice, or posting required would impede a criminal investigation or cause damage to national security, the Privacy & Security Officer or, if applicable, Business Associate will:

    a. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

    b. If the statement is made verbally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Documentation of an Incident or Breach

1. The Privacy & Security Officer and Business Associates will maintain documentation sufficient to demonstrate that

    a. for each incident, (1) the requisite investigation and/or risk assessment was conducted and (2) that all required notifications were provided; or

    b. the use or disclosure at issue did not constitute a breach of unsecured PHI (and thus no notifications were required).

2. The Privacy & Security Officer will retain documentation in accordance with the Plan's Record Retention policy.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Sections 164.400, 164.402, 164.404, 164.406, 164.408, 164.410, 164.412, and 164.414.
- The Plan's Privacy & Security Officer.
- The Plan's Record Retention Policy

- HHS website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

- FTC website on identify theft: http://www.consumer.ftc.gov/features/feature-0014-identity-theft

HIPAA POLICY AND PROCEDURE ON LIMITATIONS ON THE USE AND DISCLOSURE OF GENETIC INFORMATION

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(a)(5)(i) under the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Non-Discrimination Act of 2008 and their implementing regulations and guidance. If the HIPAA Rules are changed by HHS, the Plan will follow the revised rules.

LIMITATIONS ON USE AND DISCLOSURE OF GENETIC INFORMATION POLICY

The Plan will not use or disclose PHI that is genetic information for underwriting purposes. Genetic information includes, with respect to an individual, information about:

- The individual's genetic tests;
- The genetic tests of the individual's family members;
- The manifestation of a disease or disorder in family members (described below) of such individual; or
- Any request for, or receipt of, genetic services, or participation in clinical research, which includes genetic services, by the individual or any family member (described below) of the individual.

References to "**family members**" include: parents, spouses, siblings, children, grandparents, grandchildren, aunts, uncles, nephews, nieces, great-grandparents, great-grandchildren, great aunts, great uncles, first cousins, great-great grandparents, great-great grandchildren and children of first cousins, whether by consanguinity (such as siblings who share both parents) or affinity (such as by marriage or adoption).

In addition, references to **genetic information of an individual or family member** includes the genetic information of a fetus carried by the individual or family member, and any embryo legally held by an individual or family member using assisted reproductive technology.

Examples of prohibited use and disclosure of PHI that is genetic information for underwriting:

- A health insurance company uses an individual's family medical history or genetic test result, that was in the group health plans claims experience, to adjust the Plan's blended, aggregate premium rate for the new plan year.
- A group health plan uses an individual's family medical history that was provided as part of a health risk assessment, to provide a premium reduction to the individual. It would be permissible to request family medical history through a health risk assessment that is completed after enrollment or is unrelated to the group health plan enrollment and that is not tied to any reward or penalty.

KEY DEFINITIONS

- **Underwriting purposes** is defined broadly to include:

- Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of coverage for, benefits under the Plan. Among other items, this includes changes in deductibles or other cost sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program;

- The computation of premium or contribution amounts under the Plan. Among other items, this includes discounts, rebates, payment in kind or any other premium differential mechanisms in return for completing a health risk assessment or participating in a wellness program;

- If applicable, the application of any pre-existing condition exclusion under the Plan; and

- Other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

Underwriting purposes **do not include** determinations of medical appropriateness where an individual seeks a benefit under the Plan.

- **In Kind** refers to being paid or given goods, commodities, or services instead of money.

- **Genetic information** means:

  1. Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

     i. The individual's genetic tests;

     ii. The genetic tests of family members of the individual;

     iii. The manifestation of a disease or disorder in family members of such individual (*manifestation defined below*); or

     iv. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

  2. Any reference to genetic information concerning an individual or family member of an individual shall include the genetic information of:

     i. A fetus carried by the individual or family member who is a pregnant woman; and

     ii. Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

  3. Genetic information excludes information about the sex or age of any individual.

- **Genetic services** means:

  1. A genetic test;

  2. Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

  3. Genetic education.

- **Genetic test** means an **analysis** of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

- **Manifestation or manifested** means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. A disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

PROCEDURES

1. The Plan will not use genetic information, or request that its Business Associates use genetic information, for underwriting purposes (as that term is defined above).

2. See also the policy/procedure in this Manual on Fundraising and Underwriting.

POLICY/PROCEDURE VIOLATION

Refer to the Policy on Sanctions.

ADDITIONAL RESOURCES

- 45 CFR, Section 164.502(a)(5)(i).

- The Plan's Privacy & Security Officer.

- The Plans Policy on Fundraising and Underwriting

SECURITY POLICIES & PROCEDURES

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.308(a)(1)(ii)(A) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by Health Information Technology for Economic and Clinical Health (HITECH) Act and their implementing regulations and guidance. If the HIPAA Rules are changed by HHS, the Plan will follow the revised rules.

The Plan has no employees and, while the Plan Sponsor is entitled to receive PHI, in general, the information is required to be sent de-identified. If de-identification is not practical, minimum necessary information is sent in non-electronic media such as fax, mail, messenger or phone.

The Plan's functions, including creation and maintenance of its records, are carried out by Business Associates of the Plan. Neither the Plan nor the Plan Sponsor own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Business Associates. Accordingly, the Business Associates create, receive, maintain, and transmit all electronic PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Plan will request appropriate changes from the Business Associate if they become aware of any potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI relating to the Plan. That ability lies solely with the Plan's Business Associates.

Neither the Plan nor the Plan Sponsor have access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Business Associates affecting the security of the Plan's electronic PHI. The Plan Sponsor on behalf of the Plan has contracted with the Business Associates to require that such Business Associates undertake certain obligations relating to the security of electronic PHI that they handle in relation to the performance of administrative functions for the Plan. Therefore, the Plan's policies, and procedures, including this Policy, do not separately address the following standards (including the implementation specifications associated with them):

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;

- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

PROCEDURES

The Plan Sponsor, on behalf of the Plan, has delegated the responsibility for creating, maintaining, retaining and transmitting electronic PHI to contracted Business Associates. In compliance with Section 164.308(a)(1)(ii)(A) of the HIPAA Rules, Business Associates shall implement procedures for conducting a Risk Analysis on an ongoing basis to assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by such Business Associates. Upon request, the Business Associates will provide such procedures to the Plan.

POLICY/PROCEDURE VIOLATION

Refer to the Sanctions Policy

ADDITIONAL RESOURCES

- 45 CFR, Section 164.308(a)(1)(ii)(A).
- The Plan's Privacy & Security Officer.
- The Plan's Business Associate Policy

HIPAA POLICY AND PROCEDURE – SECURITY RISK MANAGEMENT

POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.308(a)(1)(ii)(B) of the HIPAA Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by Health Information Technology for Economic and Clinical Health (HITECH) Act and their implementing regulations and guidance. If the HIPAA Rules are changed by HHS, the Plan will follow the revised rules.

The Plan Sponsor, on behalf of the Plan, has contracted with Business Associates to administer the health benefits of its members. As such, the Plan requires and relies on its Business Associates to manage risks to electronic PHI by limiting vulnerabilities, based on risk assessments, to a reasonable and appropriate level, taking into account the following:

- Their size, complexity, and capabilities;
- Their technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and,
- The criticality of the electronic PHI potentially affected and the probability of the various risks.

PROCEDURES

Based on risk assessments undertaken by the Plan, the Plan made a reasoned, well-informed and good faith determination on the implementation of the HIPAA security regulations that it need not take any additional security measures, other than the measures set forth herein and the measures of the Business Associates, to protect against reasonably anticipated threats and vulnerabilities and to reduce risks to the confidentiality, integrity and availability of electronic PHI. Upon request, such Business Associates shall provide to the Plan their respective Risk Management plan.

POLICY/PROCEDURE VIOLATION

Refer to the Sanctions Policy

ADDITIONAL RESOURCES

- 45 CFR, Section 164.308(a)(1)(ii)(B).
- The Plan's Privacy & Security Officer.
- The Plan's Business Associate Policy