

**NATIONAL ELEVATOR INDUSTRY
HEALTH BENEFIT PLAN
PRIVACY RULES COMPLIANCE POLICY**

Effective September 23, 2013

TABLE OF CONTENTS

GENERAL PRIVACY STATEMENT	1
I. ACCESS TO PHI BY PLAN ADMINISTRATOR	2
A. General Policy	2
B. Physical Access to PHI	3
C. Storage of PHI in Plan Office.....	3
II. PERMITTED DISCLOSURE OF PHI OTHER THAN TO PLAN ADMINISTRATOR	4
A. To an Individual Requesting His Own PHI.....	4
B. To an Individual or Entity about Another Individual’s PHI	4
C. Sale or Marketing of PHI and Fundraising	12
III. REQUIRED NOTICES, FORMS AND OTHER CONSENT PROCEDURES	12
A. Notices	13
B. Authorization Forms	14
C. Cancellation of Authorization Forms	16
D. Other Consent.....	16
E. Emergencies and Disclosures After Death.....	17
IV. PROCEDURES TO DISCLOSE PERMITTED PHI	17
A. Time Limits for Processing Requests for PHI	17
B. Grants of Access to PHI	18
C. In Response to Official Requests	22
D. Denial of Access	23
E. Documentation	25
F. Accounting	25
G. Amendment	26
V. DUTIES OF TRUSTEES AS PLAN SPONSORS	27
A. Trustees as Plan Sponsors.....	27
B. Duties of Trustees	27
C. Training	28
VI. BUSINESS ASSOCIATES	28
A. Services Provided by Business Associates	28
B. Business Associate Contract	28
C. Business Associate Compliance	29
D. Unauthorized Disclosures or Other Deficiencies.....	29

VII.	COMPLAINTS REGARDING USE OR DISCLOSURE OF PHI	30
	A. Contact Person.....	30
	B. Investigation.....	30
	C. Documentation	30
	D. No Reprisal or Retaliation	30
	E. Sanctions.....	30
VIII.	UNAUTHORIZED ACQUISITION, ACCESS, USE OR DISCLOSURE OF UNSECURED PHI	31
	A. Definitions.....	31
	B. Detecting, Reporting & Investigating Unauthorized Access, Use or Disclosure of Unsecured PHI	32
	C. Notification Procedures When a Breach is Discovered	33
	D. Breach of Unsecured PHI By Plan's Business Associate.....	35
	E. Complaints Regarding Breach of PHI	36
IX.	MITIGATION POLICY.....	36
X.	SECURITY POLICY	36

EXHIBITS

- A – Authorization Form
- B – Cancellation Form
- C – Business Associate Agreement
- D – Notice of Privacy Practices
- E – Security Practices Documentation
- F – Risk Assessment Form

GENERAL PRIVACY STATEMENT

This Privacy Rules Compliance Policy (“Policy”) is intended to comply with the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rules”) issued by the Department of Health and Human Services (“HHS”) (see 45 CFR §§ 160 through 164) and promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) (42 USC § 1320d, *et seq.*). This Policy sets forth the procedures of the National Elevator Industry Health Benefit Plan (“Plan”) with respect to the use and disclosure of Protected Health Information (“PHI”) by the Plan. In general, the Plan may not use or disclose any PHI unless the person identified in the PHI consents to or authorizes the use or disclosure, or if the Privacy Rules specifically allow such use or disclosure.

PHI is any information maintained by the Plan that relates to the past, present or future physical or mental health or condition of any individual that explicitly identifies the individual or is detailed and specific enough that the identity of the individual may reasonably be determined. PHI includes the individual’s name, address, phone number, fax number, e-mail address, Social Security number, marital status, eligibility for benefits, Local Union Number, medical diagnosis, and types or dates of treatment or service. Therefore, an individual’s benefit information, claims records and benefit appeals would all include PHI. PHI may be included in mail, papers from meetings, facsimile, and electronic mail or by hand-delivery. It may or may not be identified as PHI by the distributor or sender. The use and disclosure of PHI is restricted in accordance with the provisions of this Policy. Under the applicable regulations, even looking at PHI is considered a use or disclosure of PHI.

This Policy shall govern the Plan’s and its Trustees’ access to and use, storage, transmission and disclosure of PHI. Where applicable, all persons or entities responsible for performing administrative services for the Plan (“Plan Administrator”) shall be expected to comply with this Policy and applicable law. The Plan will take all necessary corrective action and impose applicable sanctions to enforce this Policy and the requirements imposed upon it under applicable law.

Of course, not all circumstances can be covered in a policy. If you have any questions about how the Privacy Rules apply to any particular matter, you should contact the Plan’s Privacy Officer, identified below, and discuss the matter before any PHI is used or disclosed.

Privacy Officer
National Elevator Industry Health Benefit Plan
19 Campus Blvd Suite 200
Newton Square, PA 19073-3288
1-800-523-4702

I. ACCESS TO PHI BY PLAN ADMINISTRATOR

A. General Policy

1. For all purposes of this Policy, "Protected Health Information" or "PHI" shall have the same meaning as defined in 45 CFR § 160.103. Information that is otherwise PHI but concerns an individual who is deceased shall cease to be considered PHI as of 50 years after the date of the individual's death.
2. Only those employees of the Plan Administrator who process health claims for the Plan using PHI or who are otherwise authorized to have access to PHI will be assigned passwords to enable them to enter the electronic claims files and other electronic files containing PHI.
3. Only those employees described above shall have access to paper files containing PHI.
4. Employees of the Plan Administrator who do not need PHI to carry out their duties that do not require PHI shall not have access to any PHI.
5. Employees of the Plan Administrator whose duties include the handling of PHI for the Plan may not use or disclose PHI in connection with any other duties they may have as an employee of the Plan Administrator.
6. Employees of the Plan Administrator with access to PHI may not discuss, share or otherwise disclose PHI to any individual not entitled to receive access to PHI including, but not limited to:
 - a. Other employees of the Plan Administrator for any purpose except to the extent and for the purpose that the other employee has been authorized to receive that information;
 - b. A participant, beneficiary or family member of such participant or beneficiary, or any other person, in a manner inconsistent with the provisions of this Policy;
 - c. Any employer or former employer of the individual or officer and/or any employee or officer of the Union ("Union") without an executed Authorization of the individual who is the subject of the PHI (or Other Consent as applicable), and in accordance with the procedures set forth below.

7. Employees of the Plan Administrator with access to PHI may only use or disclose the minimum necessary PHI to achieve the purpose of the use or disclosure.
8. Employees of the Plan Administrator who obtain unauthorized access to PHI will be required to return or destroy the PHI and, where appropriate, may be subject to training and other correctional or disciplinary action.
9. The Plan Administrator will use and disclose PHI for treatment, payment and health care operations, and as otherwise permitted by this Policy and the Privacy Rules.

B. Physical Access to PHI

1. Only those employees who are authorized to have access to PHI to process claims or who are otherwise authorized by the Plan to enter the areas where PHI is used or stored may have physical access to these areas.
2. The Plan will take reasonable steps to assure that others (including participants and beneficiaries of the Plan, representatives of the Union, employers, and vendors, and visitors) do not have physical access to these areas.
3. All reasonable steps should be taken to insure that persons visiting the Plan Administrator's office are not exposed to or overhear discussions about PHI to which they are not entitled.

C. Storage of PHI in Plan Office

1. File cabinets containing PHI located within the Plan Administrator's office should remain closed during working hours and, to the extent that the cabinets can be locked or otherwise secured, should be locked or secured each day at the close of business.
2. To prevent disclosure of PHI within the Plan Administrator's office, any documents containing PHI that are not in file cabinets should, to the extent reasonable, be placed in folders or envelopes so that the information contained in the documents is not visible to individuals walking through the Plan Administrator's office.
3. Similarly, employees authorized to use or disclose PHI should take reasonable steps to assure that PHI, which is in use (either electronically or in written form), is similarly protected from disclosure. For instance,

whenever reasonably possible, documents containing PHI that are not in a folder or envelope should be placed facedown when not in use; likewise, PHI should not remain on computer screens when not in use and when in use should reasonably be shielded from improper disclosure.

II. PERMITTED DISCLOSURE OF PHI OTHER THAN TO PLAN ADMINISTRATOR

A. To an Individual Requesting His Own PHI

Unless otherwise excepted by this Policy or by law, the Plan will disclose an individual's PHI directly to the individual for inspection or copying upon reasonable request. A request to send PHI to a third party must be in writing and signed, and clearly identify the third party and the destination of the PHI. The Plan Administrator shall document the individual's request for disclosure of his own PHI either through receipt of a written request, completion of a form designated by the Plan Office, entry in a logbook, or through recordation in electronic form.

B. To an Individual or Entity about Another Individual's PHI

1. Spouses

- a. If an individual requests PHI relating to the individual's spouse either in writing or orally, the Plan will require a completed Authorization Form (or Other Consent under applicable circumstances) from the spouse. Upon receipt of such Authorization (or Other Consent under applicable circumstances), the Plan will disclose PHI in accordance with the procedures set forth in Section IV, below.
- b. The Plan will document the request for disclosure through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

2. Dependents other than Spouse

- a. An individual who is parent or legal guardian is entitled to access the PHI of his/her dependent minor if:
 - i. the dependent minor is less than 18 years of age;
 - ii. the dependent minor is not an emancipated minor; and

- iii. the PHI sought does not refer or relate to treatment for or advice about conditions that would under applicable state law permit the dependent minor to be treated as an adult (e.g., drug abuse, alcoholism, venereal disease, pregnancy, contraception, rape, sexual offenses).
 - b. The Plan may not disclose PHI to a parent without an Authorization Form executed by the dependent minor if the dependent minor is less than 18 years of age but:
 - i. the dependent minor is an emancipated minor; or
 - ii. the PHI sought refers or relates to treatment for or advice about conditions that would under applicable state law permit the dependent minor to be treated as an adult (e.g., drug abuse, alcoholism, venereal disease, pregnancy, contraception, rape, sexual offenses).
 - c. The Plan will document the request for disclosure through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

3. Trustees

- a. The Plan will disclose PHI to the Plan's Board of Trustees ("Trustees") only in a manner permitted by the Plan's governing documents and in accordance with this Policy. The provisions for disclosing PHI to Trustees for benefit appeals are detailed in Section II(B)(4) of this Policy. This subsection describes procedures for disclosing PHI to Trustees for other purposes.
- b. PHI may be disclosed to each Trustee (including an alternate Trustee, if applicable) either as a Board or as a subcommittee or subgroup of the Board, under the circumstances set forth below. Only the minimum amount of PHI necessary to accomplish each task will be disclosed. For the purpose of carrying out plan administration functions, PHI may be released to the Trustees under the following circumstances:
 - i. As necessary to modify, amend or terminate the Plan's plan of benefits ("Plan").
 - ii. As necessary to provide benefits under the Plan. Summary health information only will be disclosed where sufficient,

such as in the procurement of premium bids or other costs for health insurance coverage.

- iii. As necessary to decide all participant inquiries, claims and appeals referred to them. This may include pending claims and appeals as well as former claims and appeals that may be considered to determine application, interpretation and precedent.
 - iv. As necessary to monitor and determine the eligibility of participants to receive and to continue to receive accident, sickness or disability benefits under the Plan.
 - v. As necessary to interpret the provisions of the Plan.
 - vi. As necessary to enforce the provisions of the Plan, to defend against litigation brought against the Plan, or to pursue a cause of action against a participant, beneficiary, provider, or third party, for improper payment of benefits and to resolve all other claims or potential claims.
 - vii. As necessary for the Trustees to perform all obligations related to Medicare Part D and the Medicare, Prescription Drug Improvement and Modernization Act of 2003 (“MMA”), including but not limited to applying for receiving the Retiree Drug Subsidy (“RDS”).
- c. The Trustees will return to the Plan or destroy to the extent feasible, or otherwise safeguard, all PHI they receive from the Plan when no longer needed for the purpose for which they received it or as provided elsewhere in this Policy.

4. Individuals Hearing Benefit Appeals

- a. Under the Plan’s claims and appeals procedures, the Trustees, or a designated subcommittee of Trustees, are required to adjudicate appeals. The adjudication of appeals will be conducted typically in a face-to-face meeting but occasionally may be conducted by some other deliberative process, such as a teleconference, mail or facsimile. Adjudication of appeals typically involves the participation of one or more of the Plan’s Business Associates.

- b. The Plan Administrator shall be responsible for preparing any documentation necessary for the consideration of an appeal in an appeal packet in advance of the meeting or other deliberative process. Any materials that are deemed relevant to the appeal must be provided to the Plan Administrator in advance of the meeting or other deliberative process so that the materials may be prepared in accordance with the procedures set forth in Section II(B)(4)(c), below. If it becomes necessary to review additional materials relevant to the appeal that have not been included in the appeal packet, such materials must be presented to the Plan Administrator before distribution. Only Business Associates and Trustees involved in the administration of the appeals process shall be provided with the appeal packet or any supplements thereto.
- c. The appeal packet shall contain a summary of the appeal (which shall include an excerpt of the applicable Plan provision, rule or policy, and any other information required by the Plan's claims and appeals procedures), as well as back-up documentation that reasonably may be necessary for the Trustees to adjudicate the appeal. This back-up documentation may include correspondence from the claimant, medical records, and other documents containing PHI; it may also include former claims and appeals that may be relevant for the Trustees to consider in order to ensure uniform application and interpretation of the Plan. The Plan shall make a reasonable effort to eliminate all personal identifiers in the PHI contained in the appeals packet and, in any event, shall include only the minimum amount of PHI necessary to accomplish the intended purpose of considering and adjudicating the appeal. Such elimination of personal identifiers shall include the name, address, date of birth, Social Security number, participant or beneficiary plan identification number, identity of Local Union, telephone or facsimile number, electronic mail address, facial image, retiree or active status and other identifying information, unless relevant to the disposition of the appeal.
- d. After the adjudication of the appeal, all appeal packets shall be safeguarded from use or disclosure to individuals or entities not entitled to disclosure under applicable law or this Policy.

5. Union and Contributing Employers

- a. The Plan will disclose an individual's PHI to officers or employees of the Union or to an individual's employer only pursuant to an

Authorization (or Other Consent under applicable circumstances) from the individual.

- b. Upon receipt of such Authorization (or Other Consent under applicable circumstances), the Plan will disclose PHI in accordance with the procedures set forth in Section IV, below.
- c. The Plan will document the request for disclosure through an appropriate entry in a designated file or logbook, either of which may be kept in electronic format.

6. Medical Services Providers and Other Covered Entities

- a. The Plan will disclose an individual's PHI to medical service providers and other Covered Entities for the purposes of payment for services rendered for benefits provided under the Plan. Examples of payment include, but are not limited to, the following: determining coverage and benefits under the Plan; paying for or obtaining reimbursement for health care; adjudicating subrogation of health care claims or coordination of benefits; billing and collection; and making medical necessity and utilization review determinations. The Plan will only disclose the minimum necessary PHI to accomplish the purpose for which the disclosure is required.
- b. Before discussing or revealing PHI, the identity of the provider or other Covered Entity must be verified to the satisfaction of the Plan. In addition, the provider or other Covered Entity will be asked to provide the last four digits of the Social Security number or other means of verification of the individual who is the subject of the PHI.
- c. If not for the purpose of payment, the Plan will disclose PHI to medical service providers or other Covered Entities only pursuant to an Authorization. Upon receipt of such Authorization, the Plan will disclose PHI in accordance with the procedures set forth in Section IV, below.
- d. The Plan shall document the request for disclosure of PHI by medical service providers or other Covered Entities for purposes other than payment in a designated file or logbook either of which may be kept in electronic format.

7. Personal Representatives

- a. The Plan will disclose PHI to an individual's Personal Representative in the same manner as it would disclose PHI to the individual (*see* Sections II(A) and IV) but only upon receipt of documentation demonstrating that the Personal Representative has authority under applicable law to act on behalf of the individual. If the Plan has reasonable doubts about an individual's status as Personal Representative, the matter shall be referred to Plan Counsel.
- b. Notwithstanding any state law or requirement of this subsection to the contrary, the Plan may elect not to treat a person as the Personal Representative of an individual if the Plan has a reasonable belief that the individual has been or may be subjected to domestic violence or abuse or neglect by such person or treating such person as the Personal Representative could otherwise endanger the individual, and if the Plan determines in the exercise of professional judgment that it is not in the individual's best interests to treat the person as the individual's Personal Representative.
- c. If, under applicable law, an executor, administrator or other person has authority to act on behalf of a deceased individual or the individual's estate, the Plan will treat such individual as a Personal Representative under this Section with respect to the disclosure of PHI.
- d. The Plan will document the request for disclosure through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

8. Service Professionals

- a. Professional Service Providers including a third party administrator, if applicable, attorney, auditor, actuary and consultant(s) are Business Associates of the Plan. The Plan may disclose the PHI necessary for these professionals who perform services for the Plan consistent with the Business Associate Contract executed by the professional. The Plan shall only disclose the minimum necessary PHI for the professional to accomplish his service.
- b. If not for the purpose of performing contracted services for the Plan, the Plan will disclose PHI to service professionals only

pursuant to an Authorization. Upon receipt of such Authorization, the Plan will disclose PHI in accordance with the procedures set forth in Section IV, below, and will document the request for disclosure of PHI through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

9. Health/Medical Insurance Service Providers

- a. Service Providers such as claims repricing services, utilization review companies, prescription benefit manager, PPOs, and vision service managers, as applicable, are, among others, Business Associates of the Plan. The Plan may disclose the PHI necessary for these providers to perform their services for the Plan consistent with the Business Associate Contract executed by the provider. The Plan shall only disclose the minimum necessary PHI for the provider to accomplish its contracted services.
- b. If not for the purpose of providing services to the Plan, the Plan will disclose PHI to health and medical insurance service providers only pursuant to an Authorization. Upon receipt of such Authorization, the Plan will disclose PHI in accordance with the procedures set forth in Section IV, below and will document the request for disclosure of PHI through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

10. Other Insurance Providers

- a. The Plan will not disclose PHI to worker's compensation, life and disability insurance carriers unless authorized by law or pursuant to an Authorization or a Business Associate Agreement.
- b. The Plan will document the request for disclosure through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

11. Maintenance, Mechanical, Disposal and Storage Vendors

- a. Maintenance and mechanical service vendors who do not create, receive, maintain, or transmit PHI except as conduits, such as trash companies, janitorial services, mailing services, or photocopy machine repair technicians are not Business Associates. The Plan will make reasonable effort to ensure that

no PHI is disclosed to these vendors in conjunction with the performance of their services to the Plan.

- b. Those vendors who do create, receive, maintain, or transmit PHI, such as offsite storage companies or vendors responsible for the backup of electronic information or disposal of equipment or paper that may contain PHI, are Business Associates. These vendors will have access to PHI in accordance with Section VI of this Policy.

12. Schools Requiring Proof of Immunization

- a. The Plan will disclose PHI related to an individual's proof of immunization to a school required to maintain such a record by State law.
- b. The Plan will disclose such PHI upon documenting that the individual, if he is an adult or emancipated minor, or the individual's parent or guardian has provided consent, either in the form of an Authorization Form or Other Consent as described in this Policy, including a verbal authorization.
- c. The Plan will document the request for disclosure through an appropriate entry in a designated file or logbook either of which may be kept in electronic format.

13. Centers for Medicare and Medicaid Services ("CMS") (42 CFR § 423.884(b) compliance)

- a. The Plan will use and disclose PHI to CMS for any purposes required by the Trustees relating to the MMA, the Patient Protection and Affordable Care Act ("PPACA") or other applicable law.
- b. The Plan's designated Medicare Part D Authorized Representative and Account Manager will use and disclose PHI to CMS for any purposes required by the Trustees relating to the MMA, PPACA or other applicable law.
- c. Consistent with the applicable Business Associate Agreement, the Plan will permit its service providers and vendors to use and disclose PHI received from or provided to CMS for any purposes relating to the MMA, PPACA or other applicable law.

- d. As part of the training necessary to comply with their duties and responsibilities as set forth in this Policy, any individual interacting with Medicare Part D data that is also PHI will be informed:
 - i. that the information is confidential and subject to the provisions of this Privacy Policy;
 - ii. of the safeguards required by this Policy to protect the information; and
 - iii. that non-compliance with the Privacy Policy and applicable federal laws can subject those using or disclosing such Medicare Part D PHI to administrative, civil and criminal penalties.

C. Sale or Marketing of PHI and Fundraising

1. The Plan does not intend to engage in the Sale or Marketing of PHI as those terms are defined in 45 CFR § 164.502(a)(5)(ii)(B) and 45 CFR § 164.501, respectively, or to use PHI for fundraising purposes. If it engages in any of these three activities it will do so only in conformance with the HIPAA Privacy Rule and by securing the necessary participant or dependent written authorizations where required.
2. With respect to marketing, it is recognized that the following activities are not considered Marketing in accordance with 45 CFR § 164.501 and therefore are not restricted under the Privacy Rule as long as the Plan does not receive financial remuneration from a third party:
 - a. Refill reminders or other usage reminders about a current treatment, for which the Plan may be compensated by a third-party for the cost of sending the reminder;
 - b. Providing communications about alternative treatments, therapies, providers, health-related products or services available to an individual; or
 - c. Managing or coordinating care of an individual unless the Plan receives remuneration from a third party to make the communication.

3. It is recognized that the following activities are not considered to be the Sale of PHI, even if the Plan receives remuneration for them, in accordance with 45 CFR § 164.502(a)(5)(ii)(B)(2):
 - a. Use or disclosure for research, public health, treatment, payment, or other purposes required by law;
 - b. Use or disclosure made by or to a Business Associate for actions it performs as part of its agreement with the Plan to undertake certain functions;
 - c. Use or disclosure to an individual concerning that individual's PHI when requested;
 - d. Use or disclosure made as part of the sale, transfer, merger, or other consolidation of the Plan; and
 - e. Any other purpose permitted by law as long as the remuneration received is only a reasonable, cost-based fee to cover the expense to prepare and transmit the PHI, or a fee otherwise expressly permitted by other law.

III. REQUIRED NOTICES, FORMS AND OTHER CONSENT PROCEDURES

A. Notices

1. The Plan will provide, as set forth below, a Notice advising individuals covered under the Plan how medical information about the individual may be used and disclosed and how the individual may get access to this information, as follows:
 - a. To each individual covered under the Plan no later than the latest date under the law that the Plan must comply with the Privacy Rules.
 - b. To all new enrollees in the Plan at the time of enrollment.
 - c. To all individuals covered by the Plan within sixty (60) days of a material revision to the Notice.
2. No less frequently than once every three years, the Plan will notify each individual covered under the Plan of the availability of the Notice and how to obtain it.

3. Notice to the member will satisfy the requirement of notice to both the member and his dependent(s) covered under the Plan
4. The contents of the Notice will comply with the requirements of the Privacy Rules.

B. Authorization Forms

1. A valid "Authorization Form" permits the Plan to disclose PHI about an individual to someone other than the individual. A sample Authorization Form is attached as Exhibit A to this Policy, but the Plan will also honor any written authorization that the Plan determines sets forth the necessary information to allow the Plan to release PHI. The term "Authorization Form" used throughout this Policy is considered to include any such sufficient written authorization.
2. Except as otherwise permitted or required by law, the Plan may not use or disclose PHI about an individual to someone other than that individual without a valid Authorization Form. The Plan will only use or disclose PHI to the extent consistent with this Form.
3. An Authorization Form is NOT valid in any of the following circumstances:
 - a. The Plan has received a Cancellation of Authorization Form that revokes the Authorization Form.
 - b. The date on which the individual has indicated the Form will expire has already passed.
 - c. The individual has indicated an event on which the Form will expire, and the Plan knows that the expiration event has occurred.
 - d. Any material information in the Authorization Form is known by the Plan to be false.
 - e. The Authorization Form has not been filled out completely in one or more of the following ways:
 - i. The individual has not described or identified the PHI to be used or disclosed;
 - ii. The individual has not described the purpose for which the PHI is being used or disclosed, although the phrase "at the

individual's request" will suffice as a description for such purpose if the individual prefers not to describe the purpose in detail;

- iii. The individual has not provided the name (or other identification) of the person(s) to whom the Plan is to make the use or disclosure;
 - iv. The Form is not signed and dated by the individual whose PHI is the subject of the requested use or disclosure;
 - v. A Personal Representative has signed the Form and the individual has not submitted documentation to the Plan of the representative's authority to act for the individual.
4. If the individual has otherwise failed to provide information necessary for the Plan to honor the Authorization Form or otherwise failed to follow directions on the Authorization Form, the Authorization Form will be invalid. However, the Plan will contact the individual within a reasonable period of time with respect to filling out and submitting a corrected Authorization Form or the necessary information.
5. If the individual has not indicated an expiration date or expiration event on the Form, the Form will be deemed valid until the revocation of the authorization or termination by operation of law. If the individual has indicated an expiration event upon the occurrence of which the Form will expire, but the event does not relate to the individual or to the purpose of the use or disclosure, the Form will not expire as of the occurrence of that event, but will continue to be valid as described in this paragraph.
6. The Plan will not condition the provision to an individual of treatment, payment, enrollment in the Plan, or eligibility for benefits on the provision of an Authorization Form, except that the Plan may condition enrollment or eligibility for benefits on provision of an Authorization Form prior to an individual's enrollment in the Plan if the authorization is sought for the Plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations and the authorization is not for a use or disclosure of psychotherapy notes.
7. The Plan will document and retain any signed Authorization Form for six years from the date the Form was signed or last in effect, whichever is later.

8. The Plan will provide a copy of the signed Authorization Form to the individual requesting PHI and to the individual who is the subject of the PHI.

C. Cancellation of Authorization Forms

1. A valid "Cancellation of Authorization Form" cancels or revokes a previously submitted Authorization Form. A sample Cancellation Form is attached as Exhibit B to this Policy.
2. A Cancellation Form may be submitted at any time and is effective upon receipt by the Plan. The Plan will cease using or disclosing PHI to the extent consistent with the Cancellation Form.
3. A Cancellation Form is not effective to the extent that:
 - a. The Plan has taken action in reliance on the Authorization Form prior to the date the Plan receives the Cancellation Form; and/or
 - b. The Authorization Form was obtained as a condition of obtaining insurance coverage, in which case other law provides the insurer with the right to contest a claim under the policy or the policy itself.
4. The Plan will document and retain any signed Cancellation Form for six years from the date the Form was signed or last in effect, whichever is later.
5. The Plan will provide the individual with a copy of the signed Cancellation Form.

D. Other Consent

1. In the absence of an Authorization Form, the Plan may, nonetheless, disclose to an individual's family member, other relative, close personal friend, or any other person identified by the individual, the PHI related to that individual if:
 - a. the individual is present at the time of disclosure;
 - b. has the capacity to make health care decisions; and
 - c. consents in advance to the Plan's disclosure of PHI.

2. The Plan will document the Other Consent in a file or logbook either of which may be kept in electronic format.

E. Emergencies and Disclosures After Death

1. In the absence of an Authorization Form or Other Consent, the Plan may disclose PHI to an individual's family member, other relative or close personal friend under circumstance, if:
 - a. 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;
 - b. the Plan determines, in the exercise of professional judgment, that the disclosure is in the best interests of the individual; and
 - c. only the PHI that is directly relevant to the person's involvement with the individual's health care is disclosed.
2. If the individual is deceased, the Plan may disclose the PHI to an individual's family member, other relative or close personal friend that is directly relevant to such person's involvement in the individual's care unless the Plan is aware that the individual expressed a preference that the PHI not be disclosed to that person.
3. The Plan will document and log the circumstances of any disclosure made pursuant to this Section III(E).

IV. PROCEDURES TO DISCLOSE PERMITTED PHI

A. Time Limits for Processing Requests for PHI

1. The Plan will act on a request for PHI as soon as reasonably practicable but in no event later than thirty (30) days after receipt of the request unless another time frame applies, or the time period is extended as specified below. The Plan may discuss the scope, format, and other aspects of the request with the individual, as needed, to facilitate a timely response.
2. If the Plan is unable to take action within the thirty (30)-day time frame required by Section IV(A)(1) above, the Plan may extend the time for acting on a request, provided that:

- a. the extension is for no more than thirty (30) days from the end of the initial thirty (30)-day period; and
- b. prior to the expiration of the initial thirty (30)-day period, the Plan provides the individual with a written notice of the extension stating the reason(s) for the delay and the date by which the Plan will complete its action on the request.

B. Grants of Access to PHI

1. The Plan will first obtain a written request, Authorization Form, or Other Consent, as applicable, before permitting an individual access to PHI.
2. If the Plan grants a request for access to PHI, it will inform the individual of its decision and provide the type of access requested in accordance with these procedures.
3. After receiving a proper request, the Plan will provide the individual with access to PHI as it is maintained by the Plan in a “Designated Record Set” (“DRS”). A DRS consists of records or other information containing PHI that is maintained, collected, used, or disseminated by or for the Plan in connection with enrollment, claims adjudication, and case or medical management record systems maintained by the Plan, or decisions by the Plan about individuals.
4. If the same PHI that is the subject of a request is maintained in more than one DRS or at more than one location, the Plan will only produce the PHI once in response to a request.
5. The policy for handling specific types of inquiries is addressed below.

a. In-Person Inquiries

- i. When an individual first makes an inquiry, he should be cautioned not to discuss his individual questions or reveal personal information until he is escorted to a private area. However, the Plan may ask the individual to sign in and check a box on the sign-in sheet ascertaining that the individual’s inquiry involves the Plan.
- ii. The individual shall then be directed to a privacy-protected area for assistance.

- iii. Before PHI is provided to the individual, the Plan should verify the individual's identity by asking for appropriate photo identification.
- iv. Any person accompanying the individual should remain in the waiting area unless the individual wishes the other person to accompany him to the private area. In that case, the Plan must obtain either an Authorization Form or Other Consent.
- v. If the individual wishes to inspect PHI, the Plan may provide it at that time or may arrange with the individual another date and time for inspection of PHI.

b. Telephone Inquiries

- i. Before any PHI is discussed or revealed, the Plan must verify the identity of the caller by asking for information such as the last four digits of the caller's social security number, address and date of birth. The Plan may also obtain from the caller verification of the caller's identity through information the Plan has on file regarding the caller.
- ii. If the caller is requesting his own PHI, the Plan may provide the PHI to him in accordance with Section IV(B)(6) below.
- iii. If the caller is not requesting his own PHI, then no PHI may be provided unless an appropriate Authorization Form or Other Consent is obtained.

c. Fax or Mail Inquiries

- i. Before responding to a fax or mail inquiry, the Plan must verify the identity of the individual requesting PHI consistent with the steps set forth in Section IV(B)(5)(b)(i), above.
- ii. If the individual is requesting his own PHI, his request for PHI shall be provided in accordance with Section IV(B)(6) below.

- iii. If the individual is not requesting his own PHI, then no PHI may be provided unless an appropriate Authorization Form is obtained.
- d. Electronic Mail Inquiries
 - i. Before responding to an electronic mail inquiry, the Plan must verify the identity of the individual requesting PHI, consistent with the steps set forth in Section IV(B)(6)(b)(i), above.
 - ii. If the individual is requesting his own PHI, his request for PHI shall be provided in accordance with Section IV(B)(6) below.
 - iii. If the individual is not requesting his own PHI, then no PHI may be provided unless an appropriate Authorization Form is obtained.
 - iv. Requests for PHI received by e-mail and disclosures of PHI provided by e-mail should be printed and filed.
- 6. The Plan will provide an individual with the type(s) of PHI and in the form or format requested by the individual as provided below.
 - a. PHI Provided Orally
 - i. If an inquiry made by any of the methods listed in Section IV(B)(5) above is for PHI to be provided or discussed orally, after following the appropriate procedures for verifying an individual's identity or securing the necessary Authorization Form or Other Consent, the Plan may discuss such PHI.
 - b. PHI Provided in Hard Copy
 - i. If an inquiry made by any of the methods listed in Section IV(B)(5) above is for a hard copy of PHI, after following the appropriate procedures for verifying an individual's identity or securing a necessary Authorization Form or Other Consent, the Plan will provide access to the PHI in a hard copy if it can be readily produced in hard copy.

- ii. PHI provided in hard copy by the Plan to an individual may be provided by mailing it to the individual's home address, another address specified by the individual (if the request is in writing and signed) or by in-person delivery.
 - iii. The Plan may charge a reasonable fee to cover the cost of copying the hard copy (the cost of labor and supplies to be separately reported) that does not exceed charges imposed by the Plan for other types of requests for copies of documents. The Plan may also charge the individual postage if it mails the copies.
- c. PHI Provided Electronically
- i. If an inquiry made by any of the methods listed in Section IV(B)(5) above is for PHI that is maintained electronically by the Plan, after following the appropriate procedures for verifying an individual's identity, the Plan will provide the electronic PHI either in the format requested by the individual if it is easily producible to that format, or in a format agreed to between the individual and the Plan. The default format for requests for electronic PHI will be PDF.
 - ii. Before emailing or otherwise electronically providing PHI (such as by text message), the Plan must receive the individual's written or verbal permission to transmit in this medium after first informing the individual that the electronic response will be unencrypted, if applicable, and of the risks of sending unencrypted electronic messages, if applicable. In its record of the request for electronic PHI, the Plan will include a record of its disclosure of the risk of providing unencrypted PHI.
 - iii. The Plan may charge a fee for the labor costs to create, copy, compile, extract, scan or burn the electronic information as well as any electronic media used to provide the copy (such as a CD or data storage device), and for the cost of mailing the electronic media to the individual if it is mailed.
7. The Plan will not impose costs or fees, other than those specified above in connection with requests for PHI.

C. In Response to Official Requests

1. Subpoenas

- a. All subpoenas will be marked with the date and manner received.
- b. The Plan will disclose the PHI expressly requested by an order of a court or administrative tribunal.
- c. The Plan will disclose PHI in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal only under the following circumstances:
 - i. If the request is accompanied by an Authorization Form; or
 - ii. If the individual requesting the PHI supplies a written statement and accompanying documentation demonstrating that:
 - (A) the party has made a good faith attempt to provide written notice to the individual;
 - (B) the notice included sufficient information about the proceeding in which the PHI is requested; and
 - (C) the time for the individual to object has elapsed without objection being made or with all objections resolved and the disclosure of PHI sought by the party is consistent with such resolution.
 - iii. Alternatively, the individual requesting the PHI supplies a written statement and accompanying documentation demonstrating that:
 - (A) the parties to the proceeding giving rise to the request for PHI have agreed to a protective order that prohibits the parties from using the requested PHI for any purpose other than the proceeding and requires the return or destruction of the PHI (including any copies) at the conclusion of the proceeding, and have presented the protective order to the court or administrative tribunal having jurisdiction over the dispute; or

- (B) the party seeking the PHI has requested a protective order as described in the paragraph above from the court or administrative tribunal having jurisdiction over the dispute.

2. Department of Labor

The Plan will respond to informal requests for PHI by the Department of Labor (“DOL”) by obtaining DOL’s request in writing. The Plan will then forward an Authorization to the DOL and request that DOL return the valid Authorization signed by the individual who is the subject of the PHI.

3. Other Government Agencies and Public Health Officials

The Plan will comply with the applicable Privacy Rules for disclosure to governmental agencies or public health officials.

D. Denial of Access

- 1. If the Plan denies the request for access, in whole or in part, it will inform the individual of its decision with a written denial, which sets forth the following:
 - a. The basis for the denial.
 - b. If the denial is based on reviewable grounds, a statement of the individual’s review rights and a description of how the individual may exercise such rights.
 - c. A description of how the individual may complain to the Plan or to the Secretary of HHS.
 - d. In the event the Plan does not maintain the PHI that is the subject of the request for access, and the Plan knows where the requested PHI is maintained, information about where to direct the request for access.
- 2. The Plan may deny an individual's request for access without opportunity for review in one or more of the following circumstances, in accordance with 45 CFR § 164.524:
 - a. The PHI requested is for the individual's psychotherapy notes. Psychotherapy notes, as that term is used in this Policy, are notes

recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the individual's medical record. This term excludes medical prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

- b. The PHI is information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or
 - c. 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.
3. The Plan may deny a request for access in one or more of the following circumstances, provided that the individual is given a right to have such denial(s) reviewed and those rights are indicated in the denial notice as specified in this Policy detailing the procedures when access to PHI is denied:
- a. 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. 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. 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.

4. If the Plan denies access to PHI on one or more of the reviewable grounds listed in paragraph 3 immediately above, the Plan will comply with all of the following:
 - a. Provide a timely, written denial notice with the required information specified above;
 - b. Designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access, and provide the individual with a right to have the denial reviewed by such professional;
 - c. Promptly refer a request for review to such designated reviewing official. The designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested based on the standards set forth above;
 - d. Promptly provide the individual with the written determination of the designated reviewing official and take other action needed to carry out the designated reviewing official's determination; and
 - e. To the extent possible, give the individual access to any other PHI requested, after excluding the PHI to which the Plan has a ground to deny access.
5. In the event the Plan denies a request for PHI based on an unsigned or otherwise incomplete form, the Plan will comply with the time frames and other requirements set forth in this Policy.

E. Documentation

The Plan will document and retain the Designated Record Set(s) that are subject to access by individuals for at least six years from the date created or last in effect, whichever is later. The Plan will document and retain the titles of the persons or offices responsible for receiving and processing requests for access by individuals for at least six years from the date created or last in effect, whichever is later.

F. Accounting

1. An individual covered under the Plan may request the Plan to provide an accounting of disclosures of PHI made by the Plan in the six-year period prior to the date of the request. The Plan will provide the individual with

a written accounting that meets the requirements set forth in the Privacy Rules.

2. The Plan will act on the request for an accounting within sixty (60) days and may extend this time period in writing by an additional thirty (30) days. The Plan may only charge an individual for accountings in excess of one accounting in a twelve-month period.
3. In an accounting, the Plan need not include disclosures to carry out treatment, payment and health care operations, disclosures to the individual, or to others pursuant to a valid authorization, and other disclosures that are not required to be included under an accounting pursuant to the Privacy Rules. The Plan will document the request for an accounting and any action taken in response.

G. Amendment

1. An individual covered under the Plan may amend his own PHI or a record about the individual maintained by the Plan. If the PHI or record is maintained by a Business Associate or other third party known to the Plan, the Plan will make reasonable efforts to notify the third party of the amendment.
2. The Plan may deny the request to amend if the PHI or record was not created by the Plan and the creator of the PHI or record is available to make a correction, if the PHI or record is not part of a designated record set, if the PHI or record is information not available for inspection by the individual under this policy or the Privacy Rules, or if the PHI or record is accurate and complete. Any request to amend must be in writing and provide a reason to support the request to amend.
3. Within sixty (60) days, the Plan will advise the individual whether or not the request to amend is accepted or denied. This period may be extended by thirty (30) days provided the Plan informs the individual in writing of the need and reasons for the extension.
4. If the request to amend is denied, the individual has the right to submit a written statement of disagreement and this statement will be included in any future disclosures of the applicable PHI or the record by the Plan. In lieu of a statement, the individual may request the Plan to include his/her request to amend and the denial, with any future disclosures of the PHI or record. If the Plan denies the request to amend, the Plan will advise the individual of his/her right to submit a statement, to request that the request to amend and the denial accompany any future disclosures of the

PHI or record at issue, to appeal to the Plan or to complain to the Secretary of Health and Human Services. The Plan may prepare a written rebuttal to the individual's statement of disagreement and shall provide a copy of the rebuttal to the individual.

V. DUTIES OF TRUSTEES AS PLAN SPONSORS

A. Trustees as Plan Sponsors

The Trustees are the plan sponsor for the purposes of this Privacy Policy. As sponsor, it is necessary for the Trustees, either as a Board, subcommittee or subgroup of the Board, to perform certain functions that require the disclosure and use of PHI. The Trustees have amended the Plan documents to comply with the regulations promulgated by HHS pertaining to the release of PHI to the sponsor of the Plan, which in this case is the Trustees.

B. Duties of Trustees

In addition to any other applicable provisions of this Policy, the Trustees are obligated to comply with the following requirements:

1. The Trustees will not use or disclose PHI released to them for any purposes other than those permitted pursuant to this Section or as required by law. The Trustees will safeguard PHI while it is in their possession.
2. The Trustees will not disclose PHI, unless required by law or authorized by the affected participant or beneficiary, to any person other than the Business Associates of the Plan who have a right to access information through a contract with the Plan.
3. The Trustees will not use or disclose PHI for any employment-related action or decisions or in connection with any non-group health employee benefit plan they maintain as employer or union representatives.
4. The Trustees will report to the Plan any use or disclosure of PHI that is inconsistent with this Policy and applicable law so that the Plan may take appropriate steps to resolve any issues of non-compliance.
5. The Trustees will return to the Plan or destroy, to the extent feasible, all PHI they receive from the Plan when no longer needed for the purpose for which they received it.

6. Each Trustee will certify to the Plan that the Plan documents have been amended to incorporate all legal requirements for the disclosure of PHI to them and that they agree to comply with all such requirements.
7. Consistent with the applicable HHS regulations, the Trustees will make participants' or beneficiaries' own PHI available to them; will permit participants or beneficiaries an opportunity to amend PHI or individual record maintained by the Plan; and will comply with requests to the Plan by participants or beneficiaries for an accounting of disclosures of PHI.
8. The Trustees will make their internal practices, books and records relating to the use or disclosure of PHI available to the Secretary of HHS for audit purposes.
9. The Trustees will make reasonable efforts to insure that, when acting in their plan sponsor capacity, an adequate separation between them and the Plan is maintained so that confidentiality of PHI is assured.

C. Training

The Plan will provide the necessary training to ensure that the Trustees are able to comply with their duties and responsibilities as set forth in this Policy.

VI. BUSINESS ASSOCIATES

A. Services Provided by Business Associates

It is recognized that it will be necessary for the Plan to retain various firms, entities, professionals and individuals to provide services to the Plan for the proper administration of the Plan. These services include, but are not limited, to plan administration, claims processing, claims payment, data processing, billing, financial, record keeping, treatment, utilization review, quality assurance, benefit management, repricing, actuarial, legal, consulting, data aggregation, auditing and accounting. To the extent these services require the creation, receipt, maintenance, or transmission of PHI, each of these service providers will be a "Business Associate" of the Plan.

B. Business Associate Contract

Each Business Associate will be required, in a timely manner, to enter into a written contract or other written agreement or arrangement with the Plan establishing, among other things, the permitted and required uses and disclosures of PHI, the limitations on use of PHI, the required disclosure of the improper use of PHI, the proper safeguards of PHI during the term of the

contract and at its termination, and the Business Associate's responsibility in the event of a breach resulting in unauthorized use of or access to PHI. A sample Business Associate Agreement is attached as Exhibit C to this Policy.

Each Business Associate will also be required to enter into a written contract or other acceptable arrangement with any subcontractor that creates, receives, maintains, or transmits PHI of the Plan. Such a subcontractor will be considered a Business Associate of the Business Associate and must comply with all general Business Associate requirements and the same limitations on the use or disclosure of the PHI the Business Associate agrees to in its contract with the Plan. Such subcontractor will also be required to enter into a written contract or other acceptable arrangement with its subcontractors, with the same restrictions and obligations related to PHI, and such obligation will carry on through each tier of subcontractors.

The Business Associate will be required to monitor the subcontractor's compliance with its Business Associate requirements, and will report to the Plan any unauthorized or improper disclosure of PHI by the subcontractor or any lower tier of subcontractor.

C. Business Associate Compliance

No PHI will be released to a Business Associate unless the Business Associate has certified to the Plan that it has established a compliance plan to assure it will comply with the HIPAA Privacy Rules and Security Rules, and enters into a Business Associate Agreement as described above. A Business Associate will be provided with only the minimum necessary PHI to carry out the services for which it has contracted with the Plan.

Each Business Associate is directly liable for compliance with the HIPAA Security Rules and the HIPAA Privacy Rules that explicitly provide for its direct liability, as well as for any obligations included in a Business Associate Contract and/or other service agreement with the Business Associate.

D. Unauthorized Disclosures or Other Deficiencies

A Business Associate will cooperate in the Plan's monitoring of its use and disclosure of PHI and will report any unauthorized or improper disclosure of PHI. The Plan may require the Business Associate to take the action it deems necessary to correct the improper use, disclosure or maintenance of PHI and, where necessary, the Plan will terminate its relationship with a Business Associate if it determines this is necessary or prudent to protect PHI.

VII. COMPLAINTS REGARDING USE OR DISCLOSURE OF PHI

A. Contact Person

If any person learns of a use or disclosure of PHI in violation of this Privacy Policy or applicable law, the violation must be reported to the Plan's Privacy Officer. If any person receives a complaint about PHI use or disclosure, that complaint must be reported to the Plan's Privacy Officer.

B. Investigation

Any participant, beneficiary or other interested party who believes PHI has been improperly disclosed or used may file a complaint with the Privacy Officer, who has been delegated this responsibility by the Trustees. The Privacy Officer shall investigate the complaint and make a finding to the Trustees on whether or not the complaint has merit. No Trustee who is the subject of the complaint may take part in the investigation, findings or determinations.

C. Documentation

The Plan's Privacy Officer is responsible for documenting reports of any complaint about PHI or reports of violations of this Policy or applicable law. The Privacy Officer is responsible for documenting the disposition of all reports and complaints, including the imposition of sanctions.

D. No Reprisal or Retaliation

The Plan will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any person for exercising a right under the Privacy Rules or filing a complaint or report.

E. Sanctions

The Plan will apply appropriate sanctions against any person with access to PHI under this Policy who fails to comply with the Policy and applicable law. The Plan may take one or more of the following steps depending on the severity and frequency of the offense:

1. Take whatever action is necessary to protect the confidentiality of all PHI.
2. Counsel the responsible party on the legal requirements for protection of PHI and the requirements of this Policy.

3. Temporarily or permanently prevent the release of PHI to the responsible party.
4. Take steps in accordance with the Plan's governing documents to remove the responsible party.
5. Take steps in accordance with any applicable Business Associate Contract or other service provider agreement to obtain redress against the responsible party.

VIII. UNAUTHORIZED ACQUISITION, ACCESS, USE OR DISCLOSURE OF UNSECURED PHI

A. Definitions

1. "Unsecured PHI" shall mean electronic, written and spoken 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 the Health Information Technology for Economic and Clinical Health Act ("HITECH"). With respect to the Plan or a Business Associate, PHI is individually identifiable health information that is transmitted in any form or medium including electronic information (*see* 45 CFR § 160.103). If information is de-identified in accordance with 45 CFR §§ 164.514(a)-(c), it is not Protected Health Information, and thus, any inadvertent or unauthorized use or disclosure of such information will not be a Breach.
2. "Breach" means the unauthorized acquisition, access, use or disclosure of unsecured PHI in a manner not permitted by the Privacy Rules or this Policy that compromises the security or privacy of the PHI.
 - a. Any unauthorized acquisition, access, use or disclosure of unsecured PHI in a manner not permitted by the Privacy Rules or this Policy will be presumed to be a Breach unless a risk assessment conducted in accordance with Section VIII(B)(2) below determines that the PHI has not been compromised.
 - b. The term Breach excludes:
 - i. Unintentional acquisition, access or use of unsecured PHI by a workforce member or person acting under the authority of the Plan or its Business Associate, if the acquisition, access or use was made in good faith, within the scope of authority, and does not result in further

unauthorized use or disclosure in a manner not permitted by the Privacy Rules;

- ii. Inadvertent disclosure between individuals at the Plan or its Business Associate who are authorized to access unsecured PHI, provided the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Privacy Rules; or
 - iii. Disclosure of PHI where the Plan or Business Associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.
3. “Discovery of the Breach” means the first day the Breach is or, by exercising reasonable diligence, would have been known to the Plan. The Plan is 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. Discovery of the Breach occurs when the incident is first known, not when investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a “Breach” as defined in this Section VIII.

B. Detecting, Reporting and Investigating Unauthorized Access, Use or Disclosure of Unsecured PHI

1. In the event any Plan Trustee or Plan employee, representative or agent knows or suspects that there has been an impermissible use or disclosure of unsecured PHI, the employee, Trustee or other representative shall immediately make a report, in writing, to the Privacy Officer. The Privacy Officer shall maintain a logbook of all such reports.
2. Once a report has been made, the Privacy Officer shall immediately undertake a risk assessment to determine whether an impermissible use or disclosure not permitted by the Privacy Rules has occurred and whether there is a low probability that the PHI has been compromised or there is more than a low probability that the PHI has been compromised and therefore constitutes a “Breach” as defined in Section VIII(A) above. The risk assessment shall be in writing, and include:
 - a. Who received/accessed the impermissibly used/disclosed information and whether that person has an obligation to protect the information;

- b. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - c. Whether the PHI was actually acquired or viewed or if there was only an opportunity for it to be viewed;
 - d. The extent to which the risk of unauthorized access or disclosure of PHI was or has been mitigated; and
 - e. Any other factors which are relevant to a determination of Breach, as determined by the particular facts and circumstances of the use/disclosure at issue.
3. The Plan will document every risk assessment, regardless of outcome, in designated files, which will be maintained and stored in a manner designed to ensure the privacy of PHI.
 4. The Plan will provide necessary training to all employees with access to PHI and Trustees in detection and prompt reporting of possible impermissible use, access or disclosure of PHI.
 5. The Plan's Privacy Officer shall be responsible for retaining documentation of all reports of possible impermissible use, access or disclosure of PHI, risk assessments, results, and training for six (6) years.

C. Notification Procedures When a Breach is Discovered

1. If after a risk assessment it is determined that there has been a Breach, the Plan (or the Business Associate responsible for the Breach if this function has been delegated to the Business Associate as described in VIII(D)) will notify each individual whose unsecured PHI has been or is reasonably believed by the Plan (or Business Associate) to have been accessed, acquired, used or disclosed as a result of such Breach. In some cases the Plan (or Business Associate) must also notify the media and the Secretary of HHS. Such notice will be provided without unreasonable delay, and in no case later than sixty (60) calendar days after the Breach is "Discovered" as defined in Section VIII(A), above. The Privacy Officer is responsible for all notifications except to the extent that this function has been delegated to the Business Associate as described in VIII(D). The notification requirements are as follows.
2. Content of Notice to Individuals. The notification to individuals shall include, to the extent possible, the following information written in plain language:

- a. A brief description of what happened, including date of incident and date Breach was Discovered, if known;
 - b. A description of the types of unsecured PHI involved in the Breach (e.g., social security number, diagnosis, etc.), but not the actual PHI;
 - c. Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
 - d. A brief description of what the Plan (and/or Business Associate, if applicable) is doing to investigate the Breach, to mitigate harm to individuals, and to protect against future Breaches; and
 - e. The contact information for individuals to ask questions or learn additional information, which shall include a toll-free number, website, email address or postal address.
3. How to Notify Individuals. Notification to individuals whose PHI has been Breached will be sent by first class mail to the individual's last known address, unless the individual agrees to receive electronic notice. If the individual is a minor, notice will be sent to the parent or personal representative. The information may be provided in one or more mailings as information becomes available. If the Plan knows that the individual is deceased, notice will be sent to the next of kin or personal representative if the Plan has an address for either.
4. Substitute Notice to Individuals. If the Plan has insufficient or out-of-date contact information for fewer than ten (10) individuals affected by the Breach, the Plan can provide substitute notice via telephone or other means reasonably calculated to reach the individuals. If the Plan has insufficient or out-of-date contact information for ten (10) or more individuals, the Plan must provide substitute notice by either a conspicuous posting on the home page of the Plan's website for ninety (90) days or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside. Either conspicuous posting must contain a toll free number which will be active for at least ninety (90) days, where an individual can learn if his unsecured PHI may be included in the Breach.
5. Additional Urgent Notice to Individuals. If the Plan determines that a Breach may result in possible imminent misuse of the PHI, the Plan may

provide information to affected individuals by telephone or other means, in addition to providing the required notice set forth above.

6. Notification to the Media. If the Breach involves more than 500 residents of a single state or jurisdiction, the Plan (and/or Business Associate, if applicable) must notify prominent media outlets serving the state in addition to notifying the affected individuals as described above. The notice to the media must include the same content as the individual notice. It may come in the form of a press release.
7. Notification to the Department of Health and Human Services. If a Breach involves 500 people or more, regardless of whether they reside in a single state or jurisdiction, the Plan must notify the Secretary of HHS contemporaneously with the notice to individuals. When a Breach involves less than 500 people, the Plan shall maintain a log or other documentation of such Breaches and not later than sixty (60) days after the end of each calendar year shall provide the notification to the Secretary of HHS in the manner specified on the HHS website.
8. Documentation. The Plan's Privacy Officer shall be responsible for retaining all documentation relating to notification to individuals, the media and HHS for six (6) years.

D. Breach of Unsecured PHI by the Plan's Business Associate

1. The Plan's Business Associates are required to notify the Plan when they discover a Breach of unsecured PHI by the Business Associate which relates to the Plan. In some cases the Plan shall notify the affected individuals, and where applicable, the media and/or HHS, and in other cases the Business Associate will provide some of the notifications as provided in the Business Associate's Agreement. The Business Associate's notification to the Plan shall include:
 - a. Identification of each individual whose unsecured PHI the Business Associate reasonably believes has been Breached; and
 - b. Any other available information that would be necessary to provide in a required Breach notification.
2. In some cases, a Business Associate's discovery of a Breach may be imputed to the Plan. Under these circumstances, the Plan would be deemed to have "Discovered" the Breach (as defined in Section VIII(A) above) on the same day as the Business Associate discovered the Breach. If the Plan is to provide the applicable notices, it would therefore have no

more than sixty (60) days from the Business Associate's discovery of the Breach to provide notice of the Breach to affected individuals and/or the media and HHS.

3. Accordingly, where possible, the Plan's contracts with its Business Associates require its Business Associates to take the following actions to comply with the Breach Notification Rules:
 - a. Exercise reasonable diligence to promptly detect, report, conduct and document a risk assessment of any possible impermissible uses or disclosures of unsecured PHI to determine whether the use/disclosure occurred, and if so, whether it constitutes a Breach;
 - b. Notify the Plan of any Breach without unreasonable delay, upon Discovery of the Breach (as these terms are defined in the Breach Notification Rules) but in no event more than thirty (30) days from the Discovery of the Breach;
 - c. Provide a written recommendation whether the Plan or the Business Associate is in the best position to provide the required notifications; and
 - d. Unless the Plan expressly instructs otherwise, provide the affected individual(s) with notice of the Breach in compliance with the Breach Notification Rules and, to the extent permitted under the Rules, provide any other required notice in lieu of the Plan providing the notice and, confirm to the Plan that such notice has been made.

E. Complaints Regarding Breach of PHI

The provisions of the Plan's Privacy Policy regarding complaints, investigation, documentation, anti-retaliation, and sanctions shall apply to this Section VIII.

IX. MITIGATION POLICY

The Plan will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI in violation of this Policy or applicable law.

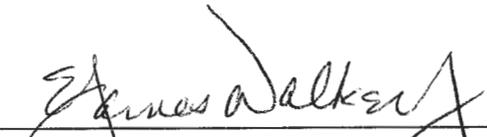
X. SECURITY POLICY

The Plan will ensure the security of electronic Protected Health Information in compliance with the Standards for Security of Electronic Protected Health Information

("Security Rules") issued by the Department of Health and Human Services (45 CFR. §§ 160, 162 and 164) and promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d, *et seq.*), as amended by Division A, Title XIII, Subtitle D, of the American Recovery and Reinvestment Act of 2009. To accomplish this end, the Plan will implement, periodically review, and modify where appropriate administrative, physical, technical and documentation safeguards that reasonably and appropriately comply with Sections 164.306, 164.308, 164.310, 164.312, 164.316 and 164.318 of the Security Rules.

This Policy is effective the 23rd day of September, 2013.

This Policy was adopted by the Board of Trustees on the 19th day of September 2013.



Chairman



Co-Chairman