

**OPERATING ENGINEERS LOCAL 139
HEALTH BENEFIT FUND**

PRIVACY RULES COMPLIANCE POLICY

TABLE OF CONTENTS

GENERAL PRIVACY STATEMENT	1
ACCESS TO PHI BY FUND ADMINISTRATOR.....	2
General Policy	2
Physical Access to PHI... ..	2
Storage of PHI.....	3
PERMITTED DISCLOSURE OF PHI OTHER THAN TO FUND ADMINISTRATOR	3
To an Individual Requesting His Own PHI.....	3
To an Individual or Entity about Another Individual’s PHI	4
Spouses.....	4
Dependents Other than Spouse	4
Trustees... ..	5
Medical Service Providers... ..	6
Personal Representatives/Attorneys... ..	6
Service Professionals.....	7
Health/Medical Insurance Service Providers... ..	7
Other Insurance Providers... ..	8
Maintenance/Mechanical Service Vendors... ..	8
Centers for Medicare and Medicaid Services.....	8
REQUIRED NOTICES, FORMS AND OTHER CONSENT PROCEDURES.....	9
Notices.....	9
Authorization Forms... ..	9
Cancellation of Authorization Forms.....	11
Other Consent.....	11
Emergencies... ..	12
PROCEDURES TO DISCLOSE PERMITTED PHI.....	12
Time Limits for Processing Requests for PHI.....	12
Grants of Access to PHI... ..	13
In-person Inquiries... ..	13
Telephone Inquiries.....	14
Fax or Mail Inquiries... ..	14
Electronic Mail Inquiries.....	14
PHI Provided Electronically.....	15
In Response to Official Requests	16
Subpoenas.....	16
Department of Labor... ..	17
Other Government Agencies and Public Health Officials... ..	17
Special Rules for Reproductive Health Care PHI (“RHC PHI”).....	17
Denial of Access... ..	19
Documentation... ..	22
Accounting	22

Amendment.....	23
BUSINESS ASSOCIATES.....	23
Services Provided by Business Associates.....	23
Business Associate Compliance.....	24
Unauthorized Disclosures or Other Deficiencies.....	24
COMPLAINTS REGARDING USE OR DISCLOSURE OF PHI.....	24
Contact Person.....	24
Investigation.....	25
Documentation.....	25
No Reprisal or Retaliation.....	25
Sanctions.....	25
UNAUTHORIZED ACQUISITION, ACCESS, USE OR DISCLOSURE OF UNSECURED PHI.....	25
Definitions.....	25
Detecting, Reporting and Investigating Unauthorized Access, Use or Disclosure of Unsecured PHI.....	26
Notification Procedures When a Breach is Discovered.....	27
Breach of Unsecured PHI by the Fund’s Business Associate.....	29
Complaints Regarding Breach of PHI.....	30
MITIGATION POLICY.....	30
SECURITY POLICY.....	30

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 U.S.C. § 1171, *et seq.*). This Policy sets forth the procedures of Fund Administrator with respect to the use and disclosure of Protected Health Information (“PHI”) by Fund Administrator. In general, Fund Administrator 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 Fund Administrator 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. Some information identified above may be maintained in files or data bases maintained by Fund Administrator but not established by or maintained by the Fund; this information is not PHI. 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.

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 Fund Administrator’s Privacy Officer, identified below, and discuss the matter before any PHI is used or disclosed.

Privacy Officer
Operating Engineers Local 139 Health Benefit Fund
N27 W23233 Roundy Drive
Pewaukee, WI 53072
(262) 549-9190

Benesys, on behalf of the Operating Engineers Local 139 Health Benefit Fund (the “Fund Administrator”) performs administrative services for various Funds, including, but not limited to, determining eligibility and processing claims. In the course of performing these duties, the Fund Administrator’s staff will have access to PHI. (These individuals will receive appropriate, timely training to ensure compliance with this Policy and applicable law.) Fund Administrator will apply appropriate sanctions against any person with access to PHI under this Policy who fails to comply with the Policy or applicable law. The Board of Trustees of the Operating Engineers Local 139 Health Benefit Fund (the “Board” of the “Plan”) adopts this Policy on its own behalf and directs that the Fund Administrator follow the Policy when performing services for the Plan.

I. ACCESS TO PHI BY FUND ADMINISTRATOR

A. General Policy

1. Only those employees of Fund Administrator who process health claims for the Fund 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 electronically.
2. Only those employees described above shall have access to paper files containing PHI.
3. Employees of Fund Administrator who do not need PHI to carry out their duties shall not have access to any PHI.
4. Employees of Fund Administrator whose duties include the handling of PHI for the Fund may not use or disclose PHI in connection with any other duties they may have as an employee of the Fund Administrator.
5. Employees of Fund 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 Fund 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 of the individual or Union officer and/or Union employee 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.
6. Employees of the Fund Administrator with access to PHI may only use or disclose the minimum necessary PHI to achieve the purpose of the use or disclosure.
7. Fund 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 Fund Administrator to enter the areas where PHI is used or stored may have physical access to these areas.

2. Fund Administrator will take reasonable steps to assure that others (including participants and beneficiaries of the Fund, union officials and/or employees, employers, vendors, and visitors) do not have physical access to these areas.
3. All reasonable steps should be taken to insure that persons visiting the Fund Administrator's office are not exposed to or overhear discussions about PHI to which they are not entitled.

C. Storage of PHI

1. File cabinets containing PHI located within Fund 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 Fund Administrator's offices, 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 Fund 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 FUND ADMINISTRATOR

A. To an Individual Requesting His Own PHI

Unless otherwise excepted by this Policy or by law, the Fund will disclose an individual's PHI directly to the individual or the individual's Personal Representative, if applicable, for inspection or copying, upon reasonable request. Fund 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 Fund 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 their spouse, Fund Administrator will require a completed Authorization Form (or Other Consent under applicable circumstances). Upon receipt of such Authorization (or Other Consent under applicable circumstances), the Fund will disclose PHI in accordance with the procedures set forth in Section IV, below.
- b. Fund Administrator will document the request for disclosure through an appropriate entry in a designated manual or electronic logbook.

2. Dependents other than Spouse

- a. An individual who is parent or legal guardian is entitled to access the PHI of their dependent minor upon receipt of a Request Form executed by the individual if:
 - i. The dependent minor is less than 18 years of age; and
 - 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. Fund Administrator may not disclose PHI 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. Fund Administrator will document the request for disclosure through an appropriate entry in a designated manual or electronic logbook.

3. Trustees

- a. Fund Administrator will disclose PHI to the various Funds' Trustees only in a manner permitted by the Fund's governing documents and in accordance with this Policy. This section will describe procedures for disclosing PHI to Trustees for other purposes.
- b. PHI may be disclosed to each Trustee and alternate Trustee, 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 Fund'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 inquires, claims and appeals that are 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 Fund Administrator or destroy, to the extent feasible, or otherwise safeguard, all PHI they receive from Fund Administrator when no longer needed for the purpose for which they received it or as provided elsewhere in this Policy.

4. Medical Services Providers

- a. Fund Administrator will disclose an individual's PHI to medical service providers 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. Fund Administrator 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 must be verified to the satisfaction of Fund Administrator. In addition, the provider will be asked to provide the last four digits of the Social Security number or alternate ID number of the individual who is the subject of the PHI.
- c. If not for the purpose of payment, Carday will disclose PHI to medical service providers only pursuant to an Authorization. Upon receipt of such Authorization, Fund Administrator will disclose PHI in accordance with the procedures set forth in Section IV, below.
- d. Fund Administrator shall document the request for disclosure of PHI by medical providers for purposes other than payment.

5. Personal Representatives/Attorneys

- a. Fund Administrator 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 Fund Administrator has reasonable doubts about an individual's status as Personal Representative, the matter shall be referred to Fund Counsel. Notwithstanding any state law or requirement of this subsection to the contrary, Fund Administrator may elect not to treat a person as the Personal Representative of an individual if Fund Administrator 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

Fund Administrator 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.

- b. 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, Fund Administrator will treat such individual as a Personal Representative under this section with respect to the disclosure of PHI.
- c. Fund Administrator will document the request for disclosure through an appropriate entry in a designated manual or electronic logbook.

6. Service Professionals

- a. The various Fund's administrator, attorney, auditor, actuary and consultant(s) are, among others, Business Associates of the Fund. Fund Administrator may disclose the PHI necessary for these professionals who perform services for the various Funds consistent with the Business Associate Contract executed by the professional. Fund Administrator 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 Fund, Fund Administrator will disclose PHI to service professionals only pursuant to an Authorization. Upon receipt of such Authorization, Fund Administrator 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 manual or electronic logbook.

7. Health/Medical Insurance Service Providers

- a. The various Funds' claims repricing services, utilization review companies, prescription benefit manager, PPOs, and vision service manager are, among others, Business Associates of the different Funds. Fund Administrator may disclose the PHI necessary for these providers to perform their services for the Fund consistent with the Business Associate Contract executed by the provider. Fund Administrator 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 Fund, Fund Administrator will disclose PHI to health and medical insurance service providers only pursuant to an Authorization. Upon receipt of such Authorization, Fund Administrator 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 manual or electronic logbook.

8. Other Insurance Providers

- a. Fund Administrator 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. Fund Administrator will document the request for disclosure through an appropriate entry in a designated manual or electronic logbook.

9. Maintenance/Mechanical Service Vendors

Fund Administrator's maintenance and mechanical service vendors, such as trash and shredding companies, janitorial services, mailing services, photocopy machine repair and off-site storage companies are not Business Associates. These vendors do not perform services that involve the use or disclosure of PHI. Therefore, no PHI will be disclosed to these vendors. Fund Administrator will make reasonable effort to ensure that any PHI disclosed to these vendors in conjunction with the performance of their services to the Fund is *de minimus*.

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

- a. Fund Administrator 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 Fund'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, Fund Administrator will permit the Fund's 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.

III. REQUIRED NOTICES, FORMS AND OTHER CONSENT PROCEDURES

A. Notices

1. Fund Administrator will utilize the forms approved by the Funds to 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 Fund 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 Fund 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 Fund Administrator to disclose PHI about an individual to someone other than the individual.
2. Except as otherwise permitted or required by law, Fund Administrator may not use or disclose PHI about an individual to someone other than that individual without a valid Authorization Form. Fund Administrator 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. Fund Administrator 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 Fund Administrator knows that the expiration event has occurred.
 - d. Any material information in the Authorization Form is known by Fund Administrator 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;
 - iii. The individual has not provided the name (or other identification) of the person(s) to whom the Fund 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 Fund of the representative's authority to act for the individual.
4. If the individual has otherwise failed to provide information necessary for Fund Administrator to honor the Authorization Form or otherwise failed to follow directions on the Authorization Form, the Authorization Form will be invalid. However, Fund Administrator 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 indicated an expiration event that 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 until the earlier of one year or the date on which the Form is signed or the date on which Fund Administrator receives a Cancellation of Authorization Form.

6. Fund Administrator 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 Fund 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. Fund Administrator will document and retain any signed Authorization Form for six (6) years from the date the Form was signed or last in effect, whichever is later.
8. Fund Administrator 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.
2. A Cancellation Form may be submitted at any time and is effective upon receipt by Fund Administrator. Fund Administrator 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. Fund Administrator has taken action in reliance on the Authorization Form prior to the date the Fund 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. Fund Administrator will document and retain any signed Cancellation Form for six (6) years from the date the Form was signed or last in effect, whichever is later.
5. Fund Administrator will provide the individual with a copy of the signed Cancellation Form.

D. Other Consent

1. In the absence of an Authorization Form, Fund Administrator may, nonetheless, disclose to an individual's family member, other relative,

close personal friend, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care 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 Fund's disclosure of PHI.
2. Fund Administrator will document the Other Consent in a manual or electronic logbook

E. Emergencies

1. In the absence of an Authorization Form or Other Consent, Fund Administrator may disclose PHI to an individual's family member, other relative or close personal friend, 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. Fund Administrator 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. Fund Administrator must document and log the circumstances of the disclosure.

IV. PROCEDURES TO DISCLOSE PERMITTED PHI

A. Time Limits for Processing Requests for PHI

1. Fund Administrator 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 Fund may discuss the scope, format, and other aspects of the request with the individual, as needed, to facilitate a timely response.
2. If Fund Administrator is unable to take action within the thirty (30)-day time frame required by Section IV (A)(1) above, Fund Administrator 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, Fund Administrator provides the individual with a written notice of the extension stating the reason(s) for the delay and the date by which they will complete its action on the request.

B. Grants of Access to PHI

1. Fund Administrator will first obtain a properly completed Request, Authorization Form, or Other Consent, as applicable, before permitting an individual access to PHI.
2. If Fund Administrator 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, Fund Administrator will provide the individual with access to PHI as it is maintained by them 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 Funds in connection with (a) the enrollment, claims adjudication, and case or medical management record systems maintained by the Fund, or (b) decisions by the Fund 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, Fund Administrator will only produce the PHI once in response to a request.
5. Fund Administrator will provide an individual with the type(s) of access to PHI and in the form or format requested by the individual, if it can be readily produced in such form or format.
6. The policy for handling specific types of access 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, Fund Administrator may ask the individual to sign in and check a box on the sign-in sheet ascertaining that the individual’s inquiry involves the Fund.
- ii. The individual shall then be directed to a privacy-protected area for assistance.

- iii. Before PHI is discussed with or revealed to the individual, Fund Administrator will verify the individual's identity by asking for appropriate picture 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, Fund Administrator must obtain either an Authorization Form or Other Consent.
- v. If the individual wishes to inspect PHI, Fund Administrator 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, must verify the identity of the caller by asking for the last four digits of the caller's social security number, address, date of birth and any other individual identifying information contained in the data maintained for our client Funds.
- ii. If the caller is requesting his own PHI, Fund Administrator may discuss PHI with him.
- iii. If the caller is not requesting his own PHI, then no PHI may be disclosed unless an appropriate Authorization Form or Other Consent is obtained.

c. Fax or Mail Inquiries

- i. Before responding to a fax or mail inquiry, Fund Administrator must verify the identity of the individual requesting PHI. PHI sent by Fund Administrator to an individual will only be provided by mailing it to the individual's home address or by in-person delivery.
- ii. If the individual is requesting his own PHI, his request for PHI shall be provided.
- iii. If the individual is not requesting his own PHI, then no PHI may be disclosed unless an appropriate Authorization Form is obtained.

d. Electronic Mail Inquiries

- i. Before responding to an electronic mail inquiry, Fund Administrator must verify the identity of the individual requesting PHI. PHI sent by Fund Administrator to an

individual will only be provided by mailing it to the individual's home address or by in-person delivery.

- ii. If the individual is requesting his own PHI, his request for PHI shall be provided.
- iii. If the individual is not requesting his own PHI, then no PHI may be disclosed 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.

e. PHI Provided Electronically

- i. An individual may request copies of PHI that is maintained electronically. After following the appropriate procedures for verifying an individual's identity, the Fund 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), Fund Administrator 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, Fund Administrator will include a record of its disclosure of the risk of providing unencrypted PHI.
 - iii. Fund Administrator 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. An individual may request copies of PHI for the time period or treatment specified by the inquiry. Fund Administrator will provide individuals with copies of the PHI requested or, if Fund Administrator cannot reasonably provide copies of the requested PHI, the Fund may provide the individual with a readable hard copy form or such other form or format as agreed to by the Fund and the individual.
8. Fund Administrator may mail copies of PHI to the individual or, alternatively, Fund Administrator and the individual may arrange for the

individual to pick up copies of the PHI at a convenient time (during regular business hours) and place.

9. Fund Administrator may charge reasonable costs of copying PHI. These costs will not exceed charges imposed by Fund Administrator for other types of requests for copies of documents. Fund Administrator may also charge the individual postage if it mails the copies. Fund Administrator will not impose costs or fees, other than those specified in this paragraph, 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. Fund Administrator will disclose the PHI expressly requested by an order of a court or administrative tribunal.
- c. Fund Administrator 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:
 - (1) The party has made a good faith attempt to provide written notice to the individual;
 - (2) The notice included sufficient information about the proceeding in which the PHI is requested; and
 - (3) 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:
 - (1) 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 presented the protective order to the court or administrative tribunal having jurisdiction over the dispute; or

- (2) 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

Fund Administrator will respond to informal requests for PHI by the Department of Labor (“DOL”) by obtaining DOL’s request in writing. Fund Administrator 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

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

4. Special Rules for Reproductive Health Care PHI (“RHC PHI”).

(a) In General. Fund Administrator will follow the HIPAA rules related to RHC PHI. This means that the Plan, and our business associates, may not use or disclose RHC PHI for any of the following activities:

- i. To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care (all as determined under 45 CFR Section 164.502);
- ii. To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care; and / or
- iii. To identify any person described in (i) or (ii).

This restriction applies only where the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and we or our business associate that received the request for RHC PHI has reasonably determined that one or more of the following conditions exists:

- y. The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided; and / or

z. The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.

In making the determinations in (y) and (z), reproductive health care provided by another person is presumed lawful unless we or our business associate has:

[1] Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided; and / or

[2] Factual information supplied by the person requesting the use or disclosure of protected health information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

(b) Specific Disclosures of RHC PHI. The Plan, and any of its business associates, may not use or disclose RHC PHI for purposes related to health oversight activities (as described in 45 CFR Section 164.512(d)), judicial or administrative proceedings (as described in 45 CFR Section 164.512(e)), law enforcement purposes (as described in 45 CFR Section 164.512(f)) or for disclosures to coroners or medical examiners (as described in 45 CFR Section 164.512(g)(1)) without obtaining an attestation that is valid from the person requesting the use or disclosure. We will use our model RHC PHI Attestation for these purposes (Reproductive Health Care Attestation Form). If we cannot use this Form, our Privacy Official will review the proposed attestation to ensure that it is valid and in compliance with HIPAA and any other applicable law.

In determining the validity of such an attestation, our Privacy Official will verify that the attestation satisfies the requirements of 45 CFR Section 164.509(b)(1) and is not “defective”. To satisfy the requirements of 45 CFR Section 164.509(b)(1), the attestation must be for a use or disclosure which is not described in (a)(i), (ii) or (iii) above.

The attestation will be “defective” if it has any of the following defects:

- i. The attestation lacks an element or statement required below, in the “Required Attestation Elements” section;
- ii. The attestation contains an element or statement not required by 45 CFR Section 164.509(c);
- iii. The attestation is combined with any other document except as allowed in 45 CFR Section 164.509(b)(3);
- iv. We or our business associate has actual knowledge that material information in the attestation is false; and / or
- v. If we or a reasonable covered entity or business associate in the same

position would not believe that the attestation is true with respect to a statement that the use or disclosure is not for a purpose prohibited by 45 CFR Section 164.502(a)(5)(iii).

In order for the attestation to be valid, it must contain the following elements:

t. A description of the information requested that identifies the information in a specific fashion, including one of the following: (A) the name of any individual(s) whose protected health information is sought, if practicable; (B) if including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose protected health information is sought;

u. The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure;

v. The name or other specific identification of the person(s), or class of persons, to whom we are to make the requested use or disclosure;

w. A clear statement that the use or disclosure is not for a purpose prohibited under 45 CFR Section 164.502(a)(5)(iii);

x. A statement that a person may be subject to criminal penalties pursuant to 42 USC Section 1320d-6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person;

y. A signature of the person requesting the protected health information (such signature may be electronic) and date. If the attestation is signed by a representative of the person requesting the information, the attestation must provide a description of such representative's authority to act for the person; and

z. The attestation must be written in plain language. It is possible that, in the course of using or disclosing RHC PHI, we were reasonably relying on a facially valid attestation and then we discover information that reasonably shows that the representation made in the attestation was false and prohibited under 45 CFR Section 164.502(a)(5)(iii). In that situation, we must cease such use or disclosure.

D. Denial of Access

1. If Fund Administrator 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 Fund or to the Secretary of HHS.
 - d. In the event Fund Administrator does not maintain the PHI that is the subject of the request for access, and Fund Administrator knows where the requested PHI is maintained, information about where to direct the request for access.
2. Fund Administrator may deny a 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 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. Fund Administrator 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 Fund Administrator denies access to PHI on one or more of the reviewable grounds listed above, Fund Administrator 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 Fund has a ground to deny access.
5. In the event Fund Administrator denies a request for PHI based on an unsigned or otherwise incomplete form, Fund Administrator will comply with the time frames and other requirements set forth in this Policy.

E. Documentation

Fund Administrator will document and retain the Designated Record Set(s) that are subject to access by individuals for at least six (6) years from the date created or last in effect, whichever is later. Fund Administrator 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 (6) years from the date created or last in effect, whichever is later.

F. Accounting

1. An individual covered under one of the various Plans may request Fund Administrator to provide an accounting of disclosures of PHI made by Fund Administrator in the six-year period prior to the date of the request. Fund Administrator will provide the individual with a written accounting that meets the requirements set forth in the Privacy Rules.
2. Fund Administrator 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. Fund Administrator may only charge an individual for accountings in excess of one accounting in a twelve-month period.
3. In an accounting, Fund Administrator need not include disclosures to carry out treatment, payment and health care operations, disclosures to the

individual, or to others pursuant to valid authorization, and other disclosures that are not required to be included under an accounting pursuant to the Privacy Rules. Fund Administrator will document the request for an accounting and any action taken in response.

G. Amendment

1. An individual covered under any of the various Plans may amend his own PHI or a record about the individual maintained by Fund Administrator. If the PHI or record is maintained by a Business Associate or other person(s) known to Fund Administrator, then Fund Administrator will make reasonable efforts to notify the third party of the amendment.
2. Fund Administrator may deny the request to amend if the PHI or record was not created by Fund Administrator 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, Fund Administrator 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 Fund Administrator 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 Fund Administrator. In lieu of a statement, the individual may request Fund Administrator to include his/her request to amend and the denial, with any future disclosures of the PHI or record. If Fund Administrator denies the request to amend, Fund Administrator 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 Fund or to complain to the Secretary of Health and Human Services. Fund Administrator may prepare a written rebuttal to the individual's statement of disagreement and shall provide a copy of the rebuttal to the individual.

V. BUSINESS ASSOCIATES

A. Services Provided by Business Associates

It is recognized that it will be necessary for the various Funds to retain various firms, entities, professionals and individuals to provide services to the Fund for the proper administration of the Fund. 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 release of PHI, each of these service providers will be “Business Associates” of the Fund.

B. Business Associate Compliance

No PHI will be released to a Business Associate unless the Business Associate has certified to the Fund that it has established a compliance plan to assure it will comply with the medical privacy requirements of HIPAA, and enters into a Business Associate Contract 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 Fund.

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.

C. Unauthorized Disclosures or Other Deficiencies

A Business Associate will cooperate in the Fund’s monitoring of its use and disclosure of PHI and will report any unauthorized or improper disclosure of PHI. The Fund 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 Fund will terminate its relationship with a Business Associate if it determines this is necessary or prudent to protect PHI.

VI. 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 Fund’s Privacy Officer or Fund Administrator’s Privacy Officer. If any person receives a complaint about PHI use or disclosure, that complaint must be reported to the Fund’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 Fund’s Privacy Officer or Fund Administrator’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

Fund Administrator 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

Fund Administrator will apply appropriate sanctions against any person with access to PHI under this Policy who fails to comply with the Policy and applicable law. Fund Administrator 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 Fund Administrator’ Collective Bargaining Agreement to remove the responsible party.
5. Take steps in accordance with any applicable Business Associate Addendum or other service provider agreement to obtain redress against the responsible party.

VII. 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 Fund 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 VII(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 Fund 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 Fund 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 Fund 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 Fund. The Fund 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 VII.

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

1. In the event any Fund Trustee or Fund Administrator 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 VII (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. Fund Administrator 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. Fund Administrator will provide necessary training to all employees with access to PHI in detection and prompt reporting of possible impermissible use, access or disclosure of PHI.
5. Fund Administrator’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 Fund (or the Business Associate responsible for the Breach if this function has been delegated to the Business Associate as described in VII(D)) will notify each individual whose unsecured PHI has been or is reasonably believed by the Fund (or Business Associate) to have been accessed,

acquired, used or disclosed as a result of such Breach. In some cases the Fund (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 VII(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 VII(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 Fund (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 Fund knows that the individual is deceased, notice will be sent to the next of kin or personal representative if the Fund has an address for either.
4. Substitute Notice to Individuals. If the Fund has insufficient or out-of- date contact information for fewer than ten (10) individuals affected by the Breach, the Fund can provide substitute notice via telephone or other means reasonably calculated to reach the individuals. If the Fund has insufficient or out-of-date contact information for ten (10) or more individuals, the Fund must provide substitute notice by either a conspicuous posting on the home page of the Fund’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 Fund determines that a Breach may result in possible imminent misuse of the PHI, the Fund 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 Fund (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 Fund must notify the Secretary of HHS contemporaneously with the notice to individuals. When a Breach involves less than 500 people, the Fund 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 Fund'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 Fund's Business Associate

1. The Fund's Business Associates are required to notify the Fund when they discover a Breach of unsecured PHI by the Business Associate which relates to the Fund. In some cases the Fund 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 Fund 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 Fund. Under these circumstances, the Fund would be deemed to have "Discovered" the Breach (as defined in Section VII(A) above) on the same day as the Business Associate discovered the Breach.

If the Fund 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 Fund’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 Fund 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 Fund or the Business Associate is in the best position to provide the required notifications; and
 - d. Unless the Fund 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 Fund providing the notice and, confirm to the Fund that such notice has been made.

E. Complaints Regarding Breach of PHI

The provisions of the Fund’s Privacy Policy regarding complaints, investigation, documentation, anti-retaliation, and sanctions shall apply to this Section VII.

VIII. MITIGATION POLICY

Fund Administrator 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.

IX. SECURITY POLICY

The Fund 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 Fund 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 1st day of December, 2024.