ALASKA ELECTRICAL HEALTH AND WELFARE FUND

Privacy Policy And Procedures

As Amended Effective June 9, 2025

TABLE OF CONTENTS

Page

I. STATEMENT OF PURPOSE 1

II. DEFINITIONS 1

III. RESPONSIBILITY FOR OVERSEEING COMPLIANCE WITH THE PRIVACY RULES 4

3.1 Responsibility of Board of Trustees. 4
3.2 Training. 4
3.3 Enforcement 4
3.4 Privacy Official 5
3.5 Privacy Contact Person 6
3.6 Facilitating Compliance 7

IV. DISCLOSURE TO BOARD OF TRUSTEES [§ 164.504(f)] 7

4.1 Overview 7
4.2 Certification of Plan Amendments 7
4.3 Permitted Uses and Disclosures 7

V. RIGHTS OF INDIVIDUALS 8

5.1 Overview and Summary of Individual Rights 8
5.2 Procedures for Communications To and From the Trust 8
5.4 Privacy Notice [§ 164.520] 9
5.5 Individual's Request for Restrictions on Use and/or Disclosure of PHI [§ 164.522] 10
5.6 Individual's Request for Confidential Communications of PHI [§ 164.522(b)] 11
5.7 Individual's Request for Access to PHI for Inspection and/or Copying [§ 164.524] 11
5.8 Individual's Request to Amend PHI [§ 164.526] 12
5.9 Individual's Request for Accounting of Disclosures [§ 164.528] 13

VI. DISCLOSURE OF PHI IN SPECIFIC SITUATIONS 14

6.1 Claim Appeals 14
6.2 Utilization, Case Management and Large Claim Reports 15
6.3 Underwriting Information 15
6.4 Psychotherapy Notes 16

VII. AUTHORIZATIONS [§ 164.508] 16

7.1 Overview 16
7.2 Permitted Disclosure Without an Authorization 16
7.3 De-Identified Information 17
7.4 Procedure 17

7.5 Revocation 17
VIII. PERSONAL REPRESENTATIVES [§ 164.502(g)] 17
8.1 Overview 17
8.2 Dependent Children 18
8.3 Incapacitated or Incompetent Individuals 18
8.4 Deceased Individuals 18
8.5 Trust's Right Not to Disclose 19
8.6 Explanation of Benefits 19
IX. DOCUMENTATION 19
9.1 Overview 19
9.2 Records Retained 19
X. BUSINESS ASSOCIATES [§ 164.504(c)] 20
10.1 Overview 20
10.2 Negotiation of Agreements 20
10.3 Minimum Necessary 20
10.4 PHI Safeguards 20
10.5 Access to Books and Records 20
10.6 Subcontractors and Agents 21
10.7 Violations 21
XI. MINIMUM NECESSARY DISCLOSURE [§ 164.502(b)] 21
11.1 Overview 21
11.2 Exceptions 21
11.3 Minimum Necessary Uses of PHI 21
11.4 Routine and Recurring Disclosures of PHI 22
11.5 Routine and Recurring Requests for PHI 22
11.6 Non-Routine Requests for PHI 22
11.7 Entire Medical Record Set 22
XII. COMPLAINTS AND MITIGATION [§ 164.530(d)] 22
12.1 Complaints 22
12.2 Mitigation 22
12.3 No Retaliation 23
XIII. BREACH OF PERSONAL HEALTH INFORMATION 23
13.1 Determination whether a Breach occurred 23
13.2 Notification in the Event of a Breach 24
13.3 Content of Notice to Individuals 24
13.4 Types of Notice provided to Individuals 25
13.5 Notice to HHS 26
13.6 Notice to Media 26
XIV. MARKETING AND SALES OF PHI 26

XV. IDENTITY VERIFICATION 26

XVI. ELECTRONIC PHI [§ 164.302, et. seq.] 26

16.1 Overview 26
16.2 Certification of Plan Amendment 27
16.3 Actions Taken in Regard to Electronic PHI 27

XVII. MISCELLANEOUS 27

17.1 Governing Law 27
17.2 Amendment 27
17.3 Interpretation 27

APPENDICES

APPENDIX A: Privacy Notice
APPENDIX B: Model Authorization Form
APPENDIX C: Model Business Associate Agreement
APPENDIX D: Summary of State Laws Governing Disclosure of a Minor's PHI

PRIVACY POLICY AND PROCEDURES

I. STATEMENT OF PURPOSE

The HIPAA Privacy Rules require that the Alaska Electrical Health and Welfare Fund not use or disclose Protected Health Information ("PHI") unless it is for Payment, Treatment or Health Care Operations or authorized by the affected Individual. Under the Privacy Rules, all disclosures of PHI shall be limited to the minimum necessary requirements.

This Policy and Procedures is enacted to document the Alaska Electrical Health and Welfare Fund's compliance with the requirements of the HIPAA Privacy Rules and to provide guidance for handling issues which may arise under the HIPAA Privacy Rules. Other Covered Entities with which the Trust contracts will follow their own privacy policies adopted pursuant to the HIPAA Privacy Rules. This Policy and Procedures will be interpreted in accordance with the governing regulations and other legal requirements.

II. DEFINITIONS

2.1 Capitalized terms not otherwise defined in this Policy shall have the meanings given to them in the HIPAA privacy regulations, 45 CFR Parts 160 and 164.

2.2 **"Breach"** means, generally, an impermissible use or disclosure of protected health information ("PHI") that compromises the security or privacy of the PHI. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors (discussed in further detail in Section XIII):

A. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

B. The unauthorized person who used the protected health information or to whom the disclosure was made;

C. Whether the protected health information was actually acquired or viewed; and

D. The extent to which the risk to the protected health information has been mitigated.

E. Exceptions to the definition of "Breach:"

1. The unintentional acquisition, access, or use of PHI by a member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority;

2. The inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized health care arrangement in which the covered

entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule; or,

3. If the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

2.3 "Business Associate" means a person or entity that:

A. On behalf of the Trust, creates, receives, maintains, or transmits protected health information for a HIPAA governed function or activity, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or

B. Provides, on behalf of the Trust, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where the provision of the service involves the disclosure of protected health information from the Trust, or from another business associate of the Trust.

2.4 "Covered Entity" means:

A. A health plan;

B. A health care clearinghouse; and,

C. A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

2.5 "Designated Record Set" means:

A. A group of records maintained by or for a Covered Entity that is:

1. The medical records and billing records about Individuals maintained by or for a covered health care provider;

2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

3. Used, in whole or in part, by or for the Covered Entity to make decisions about Individuals.

B. For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

2.6 "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

2.7 "Electronic PHI" means PHI transmitted by or maintained in electronic media.

2.8 "Individual" means the person who is the subject of PHI.

2.9 "Participant" means the employee or former employee participating in the Trust or another Individual entitled to receive a separate notice under the Privacy Rules.

2.10 "Plan Sponsor" means the Board of Trustees of the Alaska Electrical Health and Welfare Fund as the entity which establishes or maintains the Trust and its plans.

2.11 "**Protected Health Information**" (PHI) means individually identifiable health information that is maintained or transmitted by a covered entity subject to specific exclusions. PHI is individually identifiable if it is created or received by a covered entity, relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to such an individual, or the past, present, or future payment for the provision of health care to such an individual, and identifies such an individual, or there is a reasonable basis to believe the information can be used to identify the individual. **"PHI"** also encompasses the definition set forth in 45 C.F.R. § 160.103

2.12 "Policy" means this Privacy Policy and Procedures.

2.13 "Privacy Contact Person" means the individual or office designated by the Board of Trustees to receive complaints and inquiries and who can provide further information about matters covered by the Privacy Notice.

2.14 "Privacy Official" means the individual designated by the Board of Trustees to oversee compliance with the Privacy Rules and this Policy.

2.15 "Privacy Rules" means the privacy rules specified by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and detailed in 45 CFR Parts 160 and 164. References to Privacy Rules shall include any requirements established by the security regulations concerning Electronic PHI.

2.16 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

2.17 "Security Official" means the individual responsible for the development and implementation of policies and procedures required by the security regulations contained in 45 CFR Parts 160 and 164.

2.18 "Trust" means for purposes of this Policy the Alaska Electrical Health and Welfare Fund and the health plans it maintains.

2.19 "Trust Office" means the office of the Trust's administration office.

2.20 "Reportable Breach" is a Breach that must be reported to HHS and the individuals to which it pertains. A Reportable Breach may also have to be reported to the media, depending on the number of individuals whose PHI was improperly disclosed.

2.21 "Summary Health Information" means information that may be individually identifiable health information, and: (1) summarizes the claims history, claims expenses, or type of claims experienced by Individuals for whom the Plan Sponsor has provided health benefits under the Trust; and (2) from which the specific identifiers described in 45 CFR § 164.514(b)(2)(i) have been deleted.

2.22 "Workforce Members" means the Trust Office employees.

III. RESPONSIBILITY FOR OVERSEEING COMPLIANCE WITH THE PRIVACY RULES

3.1 Responsibility of Board of Trustees. The Board of Trustees of the Trust is the Plan Sponsor, plan administrator, and named fiduciary of the Trust and is responsible for overseeing the Trust's compliance with the Privacy Rules. The Board of Trustees' oversight activities will be directed and coordinated by the named Privacy Official who will work with the Trust's other advisors.

3.2 Training.

A. Trustees. All members of the Board of Trustees will receive training regarding the Trust's and their individual responsibilities under the Privacy Rules. A written training package will be produced and distributed to all Trustees. The full Board of Trustees will receive training periodically. All Trustees appointed after April 14, 2003 will receive a written training package and will meet with the Trust Attorney or Administrator to receive training. No Trustee will be allowed to receive PHI or participate in discussions where PHI may be disclosed until training under the Privacy Rules is received.

After training is completed, each Trustee will be required to sign an acknowledgement of his or her responsibility under the Privacy Rules. Records of the training will be retained by the Privacy Official.

B. Workforce Members. All workforce members of the Trust will receive training regarding the Trust's and their individual responsibilities under the Privacy Rules. All workforce members will receive training before April 14, 2003, and annually thereafter. All workforce members hired after April 14, 2003 will receive a written training package and will meet with the Trust's Privacy Official, or designee, prior to commencing their duties. At the completion 'of each training session, each workforce member will be required to sign an acknowledgement of the training received and his or her responsibility under the Privacy Rules. The Privacy Official will retain the training records of workforce members.

3.3 Enforcement. The Board of Trustees shall be responsible for enforcing the Trust's compliance with this Policy. If a violation of the Privacy Rules is discovered or disclosed, the

Trustees will take action to correct and/or mitigate the violation of the Privacy Rules or this Policy. Sanctions may include termination of the Trust's relationship with a third party or Business Associate who violates the Privacy Rules or this Policy .

Sanctions against a Trustee may include barring him or her from receiving any further PHI, requiring the Trustee to receive additional training concerning the Privacy Rules and the Trust's Privacy Policy and Procedures, reporting the Trustee's violation to the entity which appointed him or her or other sanctions which the Board of Trustees determine to be appropriate.

Violations of the Trust's privacy practices by a Business Associate's workforce member will result in disciplinary actions up to and including termination of the contract with the Trust's Business Associate.

3.4 Privacy Official.

A. Appointment. The Board of Trustees will designate a Privacy Official to oversee compliance with this Policy. The Privacy Official is:

Name:	Robert Garcia
Address:	Alaska Electrical Health & Welfare Fund 2600 Denali Street, Suite 200 Anchorage, AK 99503-2782
Telephone:	(907) 276-1246
Toll Free:	(800) 478-1246
E-mail:	Robert_g@Aetf.com

B. Responsibilities. The Privacy Official's responsibilities shall include the following:

1. Being designated as such in the Privacy Notice;

2. Receiving and answering questions and complaints related to the Privacy Rules and this Policy;

3. Providing leadership in complying with regulations related to the Trust's obligations under the Privacy Rules;

4. Monitoring compliance with the Trust's record retention requirements;

5. Serving as an internal and external liaison and resource between the Trust and outside entities (including other advisors, oversight agencies and other parties) in regard to the Trust's Privacy Policy;

6. Reporting to the Board of Trustees about compliance issues arising under the Privacy Rules, which by law or in the Privacy Official's judgment require immediate attention;

7. Reporting to the Board of Trustees on a semi-annual basis about compliance with the Privacy Rules**;**

8. Ensuring that all documentation required by the Privacy Rules is maintained pursuant to this Policy;

9. Developing systems and processes to monitor Business Associate contracts, including the return or destruction of PHI used, created, or obtained by a Business Associate upon termination of the contract (or the extension of protection if not returned or destroyed);

10. Developing systems and processes to ensure that the rights of Individuals under the Privacy Rules are observed and properly documented;

11. Other duties established by the Board of Trustees.

C. Semi-Annual Report. The Privacy Official shall report semi-annually to the Board of Trustees and shall cover the following matters:

1. Provide a general review of the Plan's Privacy Policy;

2. Suggest any recommended changes to the Policy or the Trust's procedures;

3. Identify requests made under the Privacy Rules by Individuals and the Trust's response;

4. List any complaints made under the Privacy Rules and their resolution;

5. Document compliance with the Trustee training provisions of this Policy;

6. Comment on compliance by the Trust Office with the notice and recordkeeping provisions of this Policy;

7. Report on any Security Incident or other issues related to the Trust's creation, receipt, maintenance or transmittal of Electronic PHI;

8. Address other matters requested by the Board of Trustees or deemed material by the Privacy Official.

3.5 Privacy Contact Person. The Board of Trustees will also designate a Privacy Contact Person who shall be identified in the Privacy Notice and be available to receive inquiries and complaints about the Privacy Rules. The Privacy Contact Person will serve as the backup Privacy Official in the event the Privacy Official is absent. The initial Privacy Contact Person is:

Name:	Patti Janusiewicz
Address:	Alaska Electrical Health & Welfare Fund
	701 East Tudor, Suite 200
	Anchorage, AK 99503
Telephone:	(907) 276-1246
Toll Free:	(800) 478-1246
E-mail:	patti_j@aetf.com

3.6 Facilitating Compliance. The Trustees recognize that compliance with the Privacy Rules will require differing expertise, and direct the Trust professional advisers to assist the Privacy Official in facilitating compliance.

IV. DISCLOSURE TO BOARD OF TRUSTEES [§ 164.504(f)]

4.1 Overview. The Trust will not disclose PHI to the Board of Trustees, as the Plan Sponsor, except in the manner and for the purposes specifically permitted under the Privacy Rules and this Policy. The Board of Trustees will certify before any disclosure of PHI is made that the Trust documents have been amended to comply with the Privacy Rules and that PHI will not be used for employment-related purposes.

4.2 Certification of Plan Amendments. The Board of Trustees certifies that Trust's plan documents establish the permitted uses and disclosures of PHI by the Board of Trustees and to otherwise document the Board of Trustees' compliance with the Privacy Rules.

4.3 Permitted Uses and Disclosures. The Board of Trustees as Plan Sponsor shall use or disclose PHI only in the following situations:

A. Plan administration purposes performed by the Board of Trustees on behalf of the Trust, including Payment and Health Care Operations, such as, but not limited to:

1. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing, and any other payment operations permitted by the HIPAA privacy regulations;

2. Conducting quality assessment and improvement activities, reviewing health plan performance, underwriting and premium rating, conducting or arranging for medical review, legal services, auditing, business planning and development, and any other health care operations permitted by the HIPAA privacy regulations.

B. Enrollment and eligibility information, including:

1. Coordination of benefits, adjudication or subrogation of health benefit claims;

C. Preparing and providing Summary Health Information for purposes of obtaining premium bids or setting or evaluating plan rates;

D. Preparing and providing Summary Health Information for purposes of evaluating, modifying or terminating benefits provided by the Trust;

E. PHI which an Individual authorizes the Board of Trustees to use or disclose.

4.4 Mandatory Disclosures of PHI. The Board of Trustees as Plan Sponsor shall use or disclose PHI, as required by law, or when the disclosure is made to HHS for purposes of enforcing HIPAA.

V. RIGHTS OF INDIVIDUALS

5.1 Overview and Summary of Individual Rights. This section identifies how the Trust will administer the rights provided Individuals under the Privacy Rules. These rights are:

A. Receive a Privacy Notice;

B. Request restrictions on the use and disclosure of PHI;

C. Request information be communicated in a confidential manner;

D. Request access to PHI;

E. Request to amend PHI;

F. Request an accounting of disclosures of PHI.

G. Receive notice when the individual's unsecured PHI has been inadvertently disclosed.

5.2 Procedures for Communications To and From the Trust. Unless otherwise specified, the following requirements will apply to communications to and from the Trust related to the Privacy Rules.

A. Requests must be in writing and addressed to either the Privacy Contact Person or the Privacy Official.

B. The Trust will respond within 30 days to a request for access to PHI for inspection or copying. Otherwise, the Trust will respond within 60 days of receipt of a request unless the circumstances require otherwise. The Trust may extend this time period by 30 days by notifying the Individual in writing before the end of the 60-day period, specifying the reason(s) for the delay and the date by which the Individual may expect to receive a decision on the request.

C. If a cost-based fee is charged to handle the request, the fee shall include: a charge for labor based on the current hourly rate charged by the entity providing the information for general administration services; postage; copying at the rate charged by the administrative office; and other reasonable expenses.

D. Responses to Individuals or mass mailings will be sent by first-class mail with the proof of mailing and proof of receipt saved.

E. Records of requests made by Individuals shall be retained for seven years pursuant to the Trust's record retention policies detailed in Section 9.

F. Complaints will be handled in accordance with the procedures set forth in Section 12.

5.3 Workforce Training *[§ 164.520].* The Privacy Notice will be reviewed with all workforce members during their initial training and annually thereafter.

5.4 Privacy Notice [§ 164.520].

A. Development of Privacy Notice. The Trust's Privacy Notice describes how the Trust will use and disclose PHI and an Individual's rights in regard to such information. The current Privacy Notice is attached hereto as Appendix A.

B. Distribution to Participants. For purposes of this section, the term "Participants" includes the employee or former employee participating in the Trust and an alternate payee under a Qualified Medical Child Support Order. The Privacy Notice will be provided to Participants at the following times:

1. To all new Participants with their enrollment materials. (A spouse who begins participating at a different time than the Participant will receive a separate copy of the Privacy Notice.)

2. To existing Participants within 60 days of any material revision to the Privacy Notice or upon request.

3. All current Participants will be notified at least once every three years of the availability of the Privacy Notice, and provided with instructions on how to obtain it. This information will be distributed on a triennial basis.

C. Distribution to Others. In addition to all Participants, a copy of the Privacy Notice will be provided to all Trustees**,** Business Associates and other Covered Entities with which the Trust contracts.

D. Revision of Privacy Notice. The Privacy Notice will be revised as needed to reflect any changes to this Policy. Revisions to this Policy will not be implemented prior to the effective date of the revised Privacy Notice except as required by a change in law. When revisions are necessary, all current Participants, Trustees, Business Associates and other Covered Entities with which the Trust contracts will receive a copy of the revised Privacy Notice.

E. Web Site. The Privacy Notice will be prominently displayed and available electronically on the Trust's website at http://www.aetf.com.

F. Workforce Members. The Privacy Notice will be reviewed with all workforce members during their initial training and annually thereafter.

5.5 Individual's Request for Restrictions on Use and/or Disclosure of PHI [§ 164.522].

A. Request for Restriction. Individuals may request reasonable restrictions on how the Trust uses and/or discloses their PHI for Treatment, Payment and Health Care Operations.

B. Review. Individual requests will be reviewed by the Trust's Privacy Official, or designee, for approval.

C. Approval of Request. When a request for restrictions is approved:

1. The Individual will receive notification of the approval and a statement of the effect of such a request;

2. The Privacy Official or designee will communicate the request and its approval to the Business Associates and/or Covered Entities necessary to implement the request;

3. A notation will be made in the Individual's record(s);

4. The Trust will not use or disclose PHI inconsistent with the agreed restriction;

5. The Individual will be informed that the Trust is not required to comply with the agreed upon restriction(s) in emergency treatment situations if the restricted PHI is needed for Treatment;

6. The Trust may ask the Individual to modify or revoke the restriction and get written agreement to the modification or revocation or document an oral agreement, if the agreed upon restriction hampers Treatment;

7. The use and/or disclosure of PHI of the Individual will be consistent with any approved restrictions in effect on the date it is used or disclosed.

D. Denial of Request. If a request for restriction is denied, the Individual will be given the opportunity to discuss his or her privacy concerns and, if desired efforts will be made to assist the Individual in modifying the request for restrictions to accommodate his or her concerns and obtain acceptance by the Trust.

E. Termination of a Restriction. The Trust may terminate its agreement to a restriction, if:

1. The Individual agrees to or requests the termination and it is documented in writing;

2. The Trust notifies the Individual that the agreement is being terminated, effective for PHI created or received after the notice.

F. Approval of a Restriction. The Trust will automatically approve an Individual's request to restrict the use and/or disclosure of PHI if the request is related to the treatment by a provider who has been paid in full out-of-pocket and the request is limited to the disclosure of the PHI for the purposes of carrying out payment or health care operations.

5.6 Individual's Request for Confidential Communications of PHI [§ 164.522(b)].

A. Requests for Confidential Communications. Individuals may request in writing that the Trust communicate PHI in a confidential manner. Requests should identify the reason for the request, the specific method of communication or alternative location for communication, and how the restriction is necessary to prevent a disclosure that could endanger the Individual. The Trust will accommodate such a request if administratively feasible.

B. Documentation of Requests. Written documentation of the Individual's request will be noted in the Individual's records.

C. Evaluation of Requests. Requests will be evaluated on the basis of the administrative difficulty in complying with the request and the Trust will accommodate such a request if administratively feasible.

1. It is not administratively feasible for the Trust to communicate confidentially only for a given condition, diagnosis, or treatment. All written communications to an Individual granted confidential communications will be mailed to the alternate address requested.

2. Use of an alternate address or method of communication will not terminate unless requested in writing by the Individual.

5.7 Individual's Request for Access to PHI for Inspection and/or Copying [§ 164.524].

A. Requests for Access. Individuals have the right to inspect or obtain a copy of their PHI in a Designated Record Set provided the information does not include psychotherapy notes, information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding, or is otherwise exempt from disclosure under applicable law. Individuals may request a copy of their PHI in electronic format. Individuals may also direct the Trust to transmit a copy of such PHI to an entity or person designated by the individual.

B. Response. The Trust will respond within 30 days of the request to access PHI for inspection or copying. The Trust may extend the time to provide the PHI by no more than an additional 30 days, provided that:

1. The Trust will provide a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request within 30 days of the original request.

C. Approved Request. If a request for access is approved, the Individual will be notified of the decision and may choose to inspect and/or copy the PHI in the form or format requested at a mutually agreeable place and time. At the Individual's request, the Trust will mail a copy of the requested PHI. The Trust will charge a reasonable cost-based fee for copying PHI including labor and supplies (i.e., computer disks, paper) and postage if applicable. In lieu of providing access, and if the Individual agrees in advance, the Trust may provide a summary of the requested PHI for an agreed upon additional charge. No fee will be charged, however, for retrieving or handling the PHI or for processing the Individual's access request. Notwithstanding the foregoing, the fee for a copy of an Individual's PHI in electronic format shall not be greater than the Trust's labor costs in responding to the request.

D. Denial of Request. If a request is denied, the denial of a request for access will be in accordance with the following procedures:

1. The Individual will be given a written statement that includes: the reasons for denial; if applicable, an explanation of how the Individual can have the decision reviewed; and a description of how to file a complaint with the Trust or HHS, including the title and telephone number of the Privacy Contact Person.

2. If the denial is reviewable under the Privacy Rules and the Individual requests such a review, the Trust will designate a licensed health care professional, not involved in the original denial decision, to serve as a reviewing official. Upon receipt of a review request, the Trust will promptly refer the denial to the reviewing official for reevaluation. The Trust will provide a written notice to the Individual of the reviewing official's determination.

3. If the Trust denies access because it does not maintain the PHI requested, but knows where the requested PHI is maintained, it will inform the Individual where to direct the request.

E. Discretion to Decline Access. The Trust may decline access to a personal representative of an Individual if it has a reasonable belief that the Individual has been or could be subject to domestic violence, abuse or neglect and disclosure could endanger the Individual or another person. The Trust may also decline to disclose PHI to a personal representative if it determines it is not in the best interest of the Individual to do so.

5.8 Individual's Request to Amend PHI [§ 164.526].

A. Request. Individuals may request amendment of incorrect or incomplete PHI in a Designated Record Set. The written request must include a reason to support acceptance of the amendment.

B. Acceptance of Request. If a request for amendment is accepted, in whole or in part, the Trust will identify the records that are the subject to the amendment request and will append the amendment to the records. The Trust will inform the Individual that the request

has been accepted and request the identification of and permission to contact other individuals or health care entities that need to be informed of the amendment. The Trust will make reasonable efforts to provide the amendment within a reasonable time to the persons or entities identified by the Individual as well as persons and Business Associates who the Trust knows have the disputed PHI and may rely on it to the Individual's detriment.

C. Denial of Request. A denial of a request for amendment of PHI will be processed as follows:

1. A written notice will be provided to the Individual that states the basis for denial, informs the Individual of the procedures for filing a statement of disagreement and the right to have the request and the denial included with any future release of the disputed PHI and includes a description of the procedure to file a complaint with the Trust or HHS.

2. If the Individual writes a statement of disagreement, the Trust may write a rebuttal statement and provide a copy to the Individual. The Trust shall include the request for amendment, the Trust's denial of the request, the statement of disagreement and the Trust's rebuttal (if any) with any future disclosure of the PHI.

3. If the Individual does not write a statement of disagreement, the Trust will not include the request for amendment and denial decision letter with future disclosures of the disputed PHI, unless requested by the Individual.

D. Receipt of Request from other Covered Entities. If the Trust receives notification from another Covered Entity that an Individual's PHI has been amended, the Trust will append the amendment to all applicable records of the Individual and inform its Business Associates that may use or rely on the Individual's PHI of the amendment and the need to make the necessary corrections.

5.9 Individual's Request for Accounting of Disclosures [§ 164.528].

A. Request. Individuals may request an accounting of disclosure of their PHI for disclosures in the six years prior to their request.

B. Purposes for Which an Accounting Is Not Provided. An accounting will not be provided for disclosures which were made:

1. For purposes of Treatment, Payment or Health Care Operations, including disclosures made for these purposes by any Business Associate of the Trust;

2. Pursuant to an authorization;

3. Incidental to another permissible use or disclosure;

4. To the Individual who is the subject of the information;

5. As part of a limited data set;

6. Disclosures that occurred seven years or more prior to the date of the request. .

7. For national security or intelligence purposes;

8. To correctional institutions or law enforcement officials.

C. Fee. If an Individual requests more than one accounting within the same 12-month period, the Trust may charge a reasonable, cost-based fee. The Trust will inform the Individual of the fee in advance and provide an opportunity to modify or withdraw the request.

D. Accounting. The accounting for each disclosure shall include:

1. The date of the disclosure;

2. The entity or person receiving the disclosure and their address (if known);

3. A brief description of the PHI disclosed;

4. Either a brief statement of the purpose of the disclosure, or a copy of the written request for the disclosure from HHS or from the appropriate entity;

5. If an accounting includes multiple disclosures to the same person/entity for a single purpose, the accounting will include only the frequency or number of disclosures and the date of the last disclosure made during the accounting period for all disclosures after the first disclosure.

E. Accounting by Business Associates. In responding to a request for an accounting, the Trust shall provide an accounting of disclosures made by the Trust and shall provide a list of all business associates acting on the Trust's behalf, including the business associates' most recent contact information on file. Upon request by an Individual directly to a business associate of the Trust, the business associate shall provide an accounting of the disclosures of PHI made by the business associate.

F. Accounting of Electronic Health Records. Individuals may request an accounting of disclosures of their Electronic Health Records acquired by the Trust in electronic format after January 1, 2009. Such request shall be limited to Electronic Health Records disclosed during the three years prior to the date of the request. The exclusion provided in Section 5.9B.1, regarding disclosures for treatment, payment or health care operations, shall not apply to requested accountings of Electronic Health Records.

VI. DISCLOSURE OF PHI IN SPECIFIC SITUATIONS

6.1 Claim Appeals.

A. Overview. The Board of Trustees, or a committee appointed by the Board of Trustees, is designated to hear claim appeals. The Trustees and advisors that participate in the

claim appeals will need to receive information about claim appeals to handle them appropriately. Information used and distributed in the appeal procedures will be subject to the requirements set forth below. In all circumstances, disclosures will be subject to the minimum necessary requirements.

B. Persons Receiving Claim Appeal Documents. Appeal information may be distributed to the following:

1. The claimant;

2. The claimant's personal representative if requested;

3. All Trustees who affirmatively indicate they will be present at a meeting discussing a claim appeal;

4. Trust legal counsel (if attending the hearing);

5. A representative of the claims payer involved (if attending the hearing and different than Trust Office);

6. A representative of the Trust Office;

7. The Trust consultant (if attending the hearing).

C. Method of Distribution. Documents will be mailed in envelopes marked confidential. Material will not be e-mailed or faxed unless the recipient has confirmed that appropriate steps have been taken to ensure the confidentiality of such communications.

D. Protection of PHI. Cover sheets of the appeal packets will not list the claimant's name. Unless the claimant is appearing, the information provided by the Trust Office will ordinarily exclude the "direct identifiers" listed in 45 CFR 164.514(e)(2) except for any "direct identifiers" that may be necessary to resolve the appeal. The Trust Office will also make reasonable efforts to limit the information provided to the minimum necessary to resolve the appeal, in accordance with Part XI, Section 11.1 of this Policy. Appeal Packets will be numbered with the recipient of each numbered packet identified. Packets will be returned after the conclusion of an appeal and destroyed. Copies provided to Trust Legal Counsel, the Trust Office and where applicable the claimant and his personal representative will not be destroyed.

E. Communication of Decision. Decisions on claim appeals will be mailed to the claimant or his or her personal representative in an envelope marked confidential.

6.2 Utilization, Case Management and Large Claim Reports. Utilization, case management, and large claim reports will be de-identified unless there is a specific need for disclosure of PHI, and such disclosure is consistent with the Policy and applicable law.

6.3 Underwriting Information. Information necessary for underwriting purposes, obtaining premium bids including stop loss bids, or setting and evaluating rates and benefits will

be provided as Summary Health Information unless plan administration purposes require additional disclosure and such disclosure is consistent with this Policy and applicable law.

6.4 Psychotherapy Notes.

A. Overview. Notwithstanding any other provision of this Policy, an authorization will be required to use or disclose psychotherapy notes except in the situations set forth below. For purposes of this Policy, psychotherapy notes refer to a mental health professional's notes in any medium which document or analyze the contents of a counseling session and are separated from the rest of the Individual's medical records. Psychotherapy notes do not include information regarding medication, prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests and any summary diagnosis, functioning status, the treatment plan, symptoms, prognosis and progress to date.

B. Exceptions to Authorization Requirements. The Trust will use or disclose psychotherapy notes without an authorization only to:

1. Carry out Treatment, Payment or Health Care Operations involving their use by the originator for treatment;

2. Defend itself against a legal proceeding brought by the Individual;

3. As required by law as set forth in 45 CFR § 164.512(a), § 164.512(d), § 164.512(g)(l) or § 164.512(j)(l)(i).

VII. AUTHORIZATIONS [§ 164.508]

7.1 Overview. PHI will not be disclosed without an authorization unless such disclosure is authorized by the Trust's Privacy Notice or applicable law.

7.2 Permitted Disclosure Without an Authorization. PHI will be used or disclosed without an authorization when:

A. Disclosing PHI to the Individual;

B. Disclosing information to a personal representative where applicable law does not require an authorization;

C. Using or disclosing PHI for the Trust's Treatment, Payment or Health Care Operations;

D. Disclosing PHI to a Health Care Provider for the Individual's Treatment;

E. Disclosing PHI to another Covered Entity or a Health Care Provider for that entity's Payment activities;

F. Disclosing PHI to another Covered Entity for that entity's Health Care Operations if both entities have or had a relationship with the Individual whose PHI is being requested, the PHI pertains to the current or former relationship, and the purpose of the disclosure is for: (i) a Health Care Operations activity for which the Privacy Rules state an authorization is not required; or (ii) detection of health care fraud and abuse or compliance with health care fraud and abuse laws;

G. Disclosing information to another Covered Entity that participates in an organized health care arrangement with the Trust;

H. Using PHI to create information that is not individually identifiable health information, or disclosing PHI to a Business Associate for such purpose, whether or not the de-identified information is to be used by the Trust;

I. Disclosing PHI to a Business Associate, and allowing the Business Associate to create or receive PHI on the Trust's behalf, provided the Business Associate provides satisfactory assurance that it will appropriately safeguard the information;

J. Disclosing PHI to a family member, other relative, or close personal friend of the Individual, or any other person identified by the Individual, provided the PHI is directly relevant to such person's involvement with the Individual's care or payment related to the Individual's health care, and the requirements of 45 · CFR § 164.510(b) are satisfied.

K. Otherwise using or disclosing PHI as specifically permitted by the Privacy Rules.

7.3 De-Identified Information. Information that meets the standard and implementation specifications for de-identification under 45 CFR § 164.514(a) and (b) is considered not to be individually identifiable PHI, and the requirements of this Policy shall not apply to such information. Notwithstanding the foregoing, disclosure of a code or other means of record identification designed to enable de-identified information to be re-identified constitutes disclosure of PHI. If de-identified information if re-identified, it may only be used or disclosed in accordance with this Policy and the Privacy Rules.

7.4 Procedure. If an authorization is required under this Policy, the Individual will be provided a copy and asked to sign it. Signing the authorization is voluntary and the Individual may refuse to sign it. A copy of the signed authorization shall be provided to the Individual. The Individual may revoke the authorization, in writing, at any time. The Trust's model authorization is attached as Appendix B. This shall not prevent the Trust from accepting other forms of written authorization which meet the requirements of applicable law.

7.5 Revocation. The permissions granted in the authorization shall not be acted upon if the authorization is revoked in writing or the authorized time period has expired.

VIII. PERSONAL REPRESENTATIVES [§ 164.502(g)]

8.1 Overview. A personal representative will be treated as the Individual for purposes of the Privacy Rule.

8.2 Dependent Children.

A. Dependents 18 and Over and Emancipated Minors. The PHI of a dependent 18 or older will not be disclosed without an authorization or appropriate documentation that the requestor is otherwise the Individual's personal representative such as in the case of an incapacitated minor. Emancipated minors will be treated as a dependent who is 18 or older.

B. Dependents Under 18 and Unemancipated Minors.

1. Overview. Except as limited in this Policy and under the Privacy Rules, a parent or legal guardian will be treated as the personal representative of an unemancipated minor without an authorization. As such, a parent will be allowed access to an unemancipated minor's PHI, except where a court order or other written restriction recognized by the Privacy Rules exists which limits disclosure to the requestor and has been provided to the Trust or disclosure is limited by state law. Please see Appendix D to this Policy.

2. Limitations Under State Law. The law of the state where the minor resides will control what PHI may be disclosed to a parent or legal guardian. As a general matter, disclosures involving the following will not be made to a parent or legal guardian absent the express consent of the minor:

A. The minor is 15 years or older, is living separately from parents and is financially independent from parents;

B. The minor at any age is seeking treatment for a sexually transmitted disease, including HIV/AIDS;

C. The minor at any age is seeking treatment for alcohol or substance abuse.

D. The minor is seeking mental health treatment;

E. The minor is seeking treatment related to reproductive services; or

F. There is evidence of domestic violence, abuse or neglect.

Requests involving for information involving any the foregoing shall be referred to Trust Counsel.

8.3 Incapacitated or Incompetent Individuals. The Trust will recognize personal representatives for incapacitated and incompetent Individuals pursuant to applicable state law. Court orders or other documents which are the basis for the personal representative status should be submitted with the authorization. Questions concerning the sufficiency of the submitted documentation will be referred to Trust Legal Counsel.

8.4 Deceased Individuals. The PHI of a deceased Individual will be disclosed to an individual who has authority under applicable state law to act as the executor, administrator or representative of the deceased Individual or his or her estate, provided that the requested disclosure appears reasonably related to the requestor's status as a personal representative.

Questions concerning the requestor's status as a personal representative will be referred to Trust Legal Counsel.

8.5 Trust's Right Not to Disclose. Notwithstanding the foregoing, the Trust may refuse to recognize a person as a personal representative if the Trust has a reasonable basis to believe that the Individual has been or may be subject to domestic violence, abuse or neglect by the personal representative and that treating the requesting person as a personal representative could endanger the Individual or otherwise that disclosure is not in the Individual's best interest. If the Trust refuses to recognize a personal representative, the person may request review of this refusal under the Trust's complaint procedures set forth in Section 12.

8.6 Explanation of Benefits. Explanation of benefits ("EOB") and benefit payments are part of the Trust's Payment operations, and as such may be sent to the participant or custodial parent, on behalf of the Dependent, unless the Trust determines that the information is otherwise protected.

IX. DOCUMENTATION

9.1 Overview. The Trust Office will be responsible for maintaining the records required by the Privacy Rules. The Trust's retention policies will be supervised by the Privacy Official. Records will be kept for seven years from the later of date of the record's creation or the date the record was last in effect.

9.2 Records Retained. The following records will be retained:

A. The Trust's Privacy Policy and any revisions.

B. The Trust's Privacy Notice and any subsequent revisions.

C. Plan Document Amendments.

D. Appointments of Privacy Officials and Privacy Contact Persons.

E. Business Associate Contracts.

F. Board of Trustees certifications.

G. Documentation of Trustee education.

H. Signed authorization forms.

I. Requests for restrictions on uses/disclosures of PHI.

J. Requests for confidential communications and responsive material.

K. Requests for accounting of disclosures and responsive material.

L. Requests for access and responsive material.

M. Requests for amendment of PHI and responsive material.

N. Sanctions that have been applied related to privacy violations.

O. Complaints and their disposition.

P. Communications with regulatory bodies concerning the Privacy Rules.

Q. Policies and Procedures implemented to comply with the security regulations, 45 CFR 164.302, *et. seq.*

R. A written record of any activity or assessment that is required to be documented by the security regulations, 45 CFR § 164.302, *et seq*.

S. Other documents the Privacy Official or the Board of Trustees request be maintained, or which are required to be maintained by the Privacy Rules.

X. BUSINESS ASSOCIATES [§ 164.504(c)]

10.1 Overview. Each entity contracting with the Trust will be reviewed to determine if it is another Covered Entity, a Business Associate, or neither. Business Associates will be required to enter into a separate Business Associate agreement, or an addendum to an existing agreement, which provides satisfactory assurances that the Business Associate will comply with the Privacy Rules and meets the requirements of applicable law. A model Agreement is attached hereto as Appendix C, for reference, but shall not be the mandatory form of agreement.

10.2 Negotiation of Agreements. Trust legal counsel shall be responsible for negotiating Business Associate agreements on behalf of the Trust and providing copies of such agreements to the Privacy Official.

10.3 Minimum Necessary. The Trust requires that a Business Associate determine the minimum necessary amounts and type of PHI and represent to the Trust that it has requested the minimum necessary for its purposes. The Trust relies on the professional judgment of Business Associates to determine the type and amount of PHI necessary for their purposes.

10.4 PHI Safeguards. Business Associate shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to prevent the improper use or disclosure of any PHI or electronic PHI received from or on behalf of the Trust.

10.5 Access to Books and Records.

A. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or on behalf of the Trust available to HHS or its designee for the purpose of determining the Trust's compliance with HIPAA.

B. Business Associate shall make all its Electronic Transmissions, Medical Data Code Sets, Data Conditions, Elements or Segments and Standard and Nonstandard

Transactions, and any Trading Partner Agreements relating to the Transmission or Translation of Electronic Media for which the HHS has adopted a Standard or Code Set or Data Condition, Element or Segment under 45 CFR § 162, either conducted, received, or translated by Business Associate on behalf of the Trust available to HHS or its designee for the purpose of determining Business Associate's compliance with the EDI Rules. Business Associate will certify to the Trust or to HHS or its designee that it is in compliance with the EDI Rules in accordance with 45 CFR § 162 and any further rule or regulation promulgated after the Business Associate Agreement is executed.

10.6 Subcontractors and Agents. Business Associate shall require each of its subcontractors or agents that create, receive, maintain, or transmit PHI on behalf of the Trust to agree to written contractual provisions that impose the same obligations to protect such PHI as are imposed on Business Associate by the Trust's Business Associate Agreement.

10.7 Violations. Violations of the Privacy Rules by a Business Associate, in the form of a Breach or Security Incident, shall be reported to the Privacy Official. The Privacy Official shall review the complaints and determine if there is a reasonable basis for believing a violation has occurred. If there is a reasonable basis for believing a violation has occurred, the Privacy Official shall confer with Trust Legal Counsel and report the matter to the Board of Trustees with a recommendation for any corrective action or mitigation. If correction or mitigation is unsuccessful, the Board of Trustees shall determine whether termination of the agreement is feasible.

XI. MINIMUM NECESSARY DISCLOSURE [§ 164.502(b)]

11.1 Overview. When using or disclosing PHI, or when requesting PHI from another Covered Entity, the Trust, the Board of Trustees, its Business Associates and entities participating in an organized health care arrangement with the Trust will limit PHI, to the extent practicable, to a Limited Data Set as defined by 45 U.S.C. § 164.514(e)(2) or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request in accordance with guidance provided by the Secretary of the Department of Health and Human Services.

11.2 Exceptions. The minimum necessary standard does not apply to:

A. Disclosures to or requests by a Health Care Provider for Treatment;

B. Uses or disclosures made to the Individual or his or her personal representative;

C. Uses or disclosures made pursuant to an authorization;

D. Disclosures to the Secretary of HHS pursuant to the Privacy Rules; and

E. Uses or disclosures otherwise required by law.

11.3 Minimum Necessary Uses of PHI. The Trust Office has identified workforce members, Business Associates, Trustees, etc., who need access to PHI according to the categories of uses for payment or health care operations and has also identified the type and minimum

amount of PHI needed to administer the Plan. The Trust has determined the circumstances under which individuals who perform plan functions may use PHI. All individuals are required to use PHI in accordance with the determination made by the Trust Office of the minimum amount necessary to effectively administer the Plan. When an individual performs more than one function, the types of PHI and conditions of access are dependent on the function that the individual is performing.

11.4 Routine and Recurring Disclosures of PHI. The Trust has identified disclosures of PHI it makes on a routine and recurring basis and has determined the minimum amounts of PHI necessary to achieve the purpose of these requests.

11.5 Routine and Recurring Requests for PHI. The Trust has identified requests for PHI it makes on a routine and recurring basis and has determined the minimum amount of PHI needed to achieve the purpose of these requests.

11.6 Non-Routine Requests for PHI. Requests for non-routine disclosure of PHI from another Covered Entity or Business Associate will be reviewed by the Privacy Official on a case-by-case basis to ensure that the amount of PHI requested is the minimum necessary to achieve the purpose of the request. The Trust may rely on representations that the PHI requested is the minimum necessary if the request is for a use or disclosure permitted under the Privacy Rules and is from a public official, Health Care Provider or a professional providing services to the Trust who is a Business Associate and who represents in writing that the PHI requested is the minimum necessary to perform services for the Trust.

11.7 Entire Medical Record Set. The Trust will not use, request, or disclose the entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

XII. COMPLAINTS AND MITIGATION [§ 164.530(d)]

12.1 Complaints. Any person may make complaints concerning the Trust's compliance with the Privacy Rules or this Policy or the application of this Policy in a particular situation. Complaints must be in writing and directed to the Privacy Official or Privacy Contact Person. The Privacy Official will investigate any complaint in conjunction with any Trust advisers or providers whose involvement is necessary to evaluate the complaint. The Privacy Official will respond within the 60-day time period provided under Section 5.2B of this Policy.

The Privacy Official will inform the Board of Trustees of all complaints, the results of the Privacy Official's review and any recommended corrective action or mitigation. The Board of Trustees is authorized to act on the Privacy Official's review and recommendations concerning a particular complaint. The person who has complained will be informed in writing of the Trust's decision.

12.2 Mitigation. The Trust will mitigate, to the extent practicable, any harmful effect that is known to the Trust of a use or disclosure of PHI in violation of the Trust's policies and procedures or the requirements of the Privacy Rules by the Trust or a Business Associate.

12.3 No Retaliation. The Trust will not intimidate, coerce, or retaliate against any Individual who makes a complaint to the Trust or to HHS, provides testimony, assists in investigations or chooses to exercise any of the rights granted by the Privacy Rule.

XIII. BREACH OF PERSONAL HEALTH INFORMATION

13.1 Determination whether a Breach Occurred. Acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the privacy rules is presumed to be a Reportable Breach, unless the Privacy Official determines that there is a low probability that the privacy or security of the PHI has been or will be compromised.

The Privacy Official's determination of whether a Reportable Breach has occurred must include the following considerations:

A. Was there a violation of HIPAA Privacy Rules? There must be an impermissible use or disclosure in connection with PHI by the Trust, a Business Associate of the Trust or a subcontract of a Business Associate. Impermissible use or disclosure includes theft, hacking, and other acts performed by third parties that provide the third party unauthorized access to PHI. If no impermissible use or disclosure, then the notice requirements do not apply.

B. Was PHI involved? If not, then the notice requirements do not apply.

C. Was the PHI secured? For electronic protected health information to be "secured," it must have been encrypted to NIST standards or destroyed. For paper protected health information to be "secured," it must have been destroyed. If yes, then the notice requirements do not apply.

D. Was there unauthorized access, use, acquisition, or disclosure of PHI? A HIPAA Privacy violation must involve the unauthorized access, use, acquisition, or disclosure of PHI. Otherwise, there is no violation. Examples include, but are not limited to: was PHI sent to the wrong recipient? Was the Trust's computer database hacked? Did an employee of a business associate take financial information of trust participants?

E. Is there a low probability that privacy or security was compromised? If the Privacy Official determines there is a low probability of compromise, then the notice requirements do not apply. To determine whether there is only a low probability that the privacy or security of the PHI was compromised, the Privacy Official must perform a risk assessment that considers at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud; did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual or otherwise to further the unauthorized recipient's own interests.

2. The unauthorized person who used the protected health information or to whom the disclosure was made. For example, does the unauthorized recipient of PHI have obligations to protect the privacy and security of the protected health information? Would those obligations lower the probability that the recipient would use or further disclose the PHI inappropriately? Also, was the PHI impermissibly used within a covered entity or business associate, or was it disclosed outside a covered entity or business associate?

3. Whether the PHI was actually acquired or viewed. If there was only an opportunity to actually view the information, but the Privacy Official determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise.

4. The extent to which the risk to the PHI has been mitigated. If the Trust can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient of that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

If the Privacy Official determines that there is only a low probability that the privacy or security of the information was compromised, then the Trust will document the determination in writing, keep the documentation on file, and not provide notifications. On the other hand, if the Privacy Official is not able to determine that there is only a low probability that the privacy or security of the information was compromised, the Trust will provide notifications.

13.2 Notification in the Event of a Breach. In the event a Breach or unauthorized disclosure of PHI by the Trust or one of its Business Associates is discovered, the Privacy Official, the Board of Trustees and the Trust's legal counsel shall be notified. The Trust shall provide notice to each Individual affected by the Breach, as well as the Department of Health and Human Services and local media, as required by law. Such notice shall describe the Breach, the type of information disclosed, the steps the Trust is taking to mitigate the Breach and the steps Individuals can take to protect themselves. The notice will be provided within 60 days of the date the Breach is discovered.

13.3 Content of Notice to Individuals. Notices to individuals will be written in plain language and contain all of the following, to the extent available:

A. A brief description of the incident.

B. If known, the date of the Breach and the Discovery Date.

C. A description of the types of unsecured PHI involved (for example, full name, Social Security numbers, address, diagnosis, date of birth, account number, disability code, or other).

D. The steps individuals should take to protect themselves (such as contacting credit card companies and credit monitoring services).

E. A description of what the Trust or Business Associate is doing to investigate the Breach, such as filing a police report or reviewing security logs or tapes.

F. A description of what the Trust is doing to mitigate harm to individuals.

G. A description of what measures the Trust is taking to protect against further breaches (such as sanctions imposed on the Business Associate involved in the Breach, encryption, installation of new firewalls).

H. Contact information for individuals to learn more about the Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

13.4 Types of Notice provided to Individuals. The Trust will deliver individual notices using the following methods, depending on the circumstances of the breach and the Trust's contact information for affected individuals.

A. Actual Notice. The Trust will provide actual notice in all cases, unless the Trust has insufficient or out-of-date addresses for the affected individuals. Actual written notice-

1. will be sent via first-class mail to last known address of the individual(s);

2. may be sent via email instead, if the individual has agreed to receive electronic notices;

3. will be sent to the parent on behalf of a minor; and

4. will be sent to the next-of-kin or personal representative of a deceased person, if the Trust knows the individual is deceased and has the address of the next-of-kin or personal representative.

B. Substitute Notice. The Trust will provide substitute notice if it has insufficient or out-of-date addresses for the affected individuals.

1. If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, an alternate written notice, or other means.

2. If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.

C. Substitute notice via website. Conspicuous posting on home page of the website of the Trust or Trust Sponsor for 90 days, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. Contents of the notice can be provided directly on the website or via hyperlink.

D. Substitute notice via media. Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach.

1. Substitute Notice is not required if the individual is deceased and the Trust has insufficient or out-of-date information that precludes written notice to the next-of-kin or personal representative of the individual.

E. Urgent Notice. The Trust will provide urgent notice, in addition to other required notice, in circumstances where imminent misuse of unsecured PHI may occur. Urgent notice must be given by telephone or other appropriate means.

13.5 Notice to HHS. Notice of all Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

A. Immediate Notice to HHS. If the Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

B. Annual Report to HHS. The Privacy Official will maintain a log of Breaches that involve fewer than 500 affected individuals, and will report to HHS the Breaches that were discovered in the preceding calendar year. The reports are due within 60 days after the end of the calendar year. The reports will be submitted as directed on the HHS website.

13.6 Notice to Media. Notice to media (generally in the form of a press release) will be given if a Breach affects more than 500 residents of any one state or jurisdiction. If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for giving notice to media.

13.7 Notice to State Officials. Notice to State of Alaska shall be given if required under AS 45.48.010 *et seq*.

XIV. MARKETING AND SALES OF PHI

The Trust will not engage in marketing as defined by the Privacy Rules or the sale of PHI. The Trust shall ensure that its Business Associates comply with all restrictions on marketing and the sale of PHI.

XV. IDENTITY VERIFICATION

Prior to disclosing PHI, the Trust will verify the identity of the Individual pursuant to procedures established by the Trust Office. Business Associates who routinely receive telephone calls from Participants for the Trust shall establish procedures for verifying the identity of Individuals calling and shall inform the Trust of these procedures.

XVI. ELECTRONIC PHI [§ 164.302, et. seq.]

16.1 Overview. The Board of Trustees will oversee the Trust's compliance with the security standards concerning Electronic PHI under 45 CFR §164.302, et. seq. The Board of

Trustees' oversight activities will be directed and coordinated by the named Privacy Official who will work with the Trust's Business Associate.

16.2 Certification of Plan Amendment. The Board of Trustees certifies it has amended the Trust's plan documents to provide that the Board of Trustees, as Plan Sponsor, will reasonably and appropriately safeguard Electronic PHI created, received, maintained, or transmitted to or by the Trustees on behalf of the Trust.

16.3 Actions Taken in Regard to Electronic PHI. The Trust shall take the following action in regards to Electronic PHI:

A. Ensure Confidentiality, Integrity and Availability. The Trust shall ensure the confidentiality, integrity and availability of all Electronic PHI that the Trust creates, receives, maintains or transmits.

B. Protection Against Anticipated Threats. The Trust will protect against any reasonably anticipated threats or hazards to the security or integrity of Electronic PHI.

C. Protection Against Unauthorized Disclosures. The Trust shall protect against any reasonably anticipated uses or disclosures of Electronic PHI that are not permitted or required under applicable law.

D. Contracts with Business Associates. Business Associates that may create, receive, maintain or transmit Electronic PHI must agree to written contractual provisions which impose at least the same obligations in regard to Electronic PHI as apply to the Trust and must agree to otherwise meet the requirements of 45 CFR §164.314(a).

E. Reporting Security Incidents. The Board of Trustees collectively, and each Trustee individually, will report to the Trust any Security Incident of which it or the individual Trustee becomes aware.

F. Security Official. The Privacy Official appointed by the Trust shall also serve as Security Official.

XVII. MISCELLANEOUS

17.1 Governing Law. This Policy shall be governed by Alaska law to the extent not preempted by federal law.

17.2 Amendment. The Board of Trustees may amend this Policy by written amendment.

17.3 Interpretation. The Board of Trustees has discretion to interpret the terms of this Policy and to handle issues not specifically addressed herein. This Policy will be interpreted in a manner to assure compliance with applicable law.

Dated this 9th day of June, 2025.

Chairman

Secretary

Appendix A

ALASKA ELECTRICAL HEALTH & WELFARE FUND
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. **PLEASE REVIEW IT CAREFULLY.**

Pursuant to regulations issued by the federal government, the Alaska Electrical Health and Welfare Fund is providing you this Notice about the possible uses and disclosures of your health information. Your health information is information that constitutes protected health information as defined in the Privacy Rules issued by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

As required by law, the Fund has established a policy to guard against unnecessary disclosure of your health information. The Fund is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured health information.

This Notice describes the circumstances under which and the purposes for which your health information may be used and disclosed and your rights with regard to such information.

I. Use and Disclosure of Health Information

Your health information may be used and disclosed without an authorization in the following situations:

A. To Make or Obtain Payment. The Fund may use or disclose your health information to make payment to or collect payment from third parties, such as other health plans or providers, for the care you receive, to determine benefit responsibility under the Fund's Plan or to coordinate Plan coverage. For example, the Fund may use health information to pay your claims or share information regarding your coverage or health care treatment with other health plans to coordinate payment of benefits. The Fund may also share your protected health information with another entity to assist in the adjudication or reimbursement of your health claims.

B. To Facilitate Treatment. The Fund may disclose information to facilitate treatment which involves providing, coordinating or managing health care or related services. For example, the Fund may disclose the name of your treating physician to another physician so that the physician may ask for your x-rays.

C. To Conduct Health Care Operations. The Fund may use or disclose health information for its own operations, to facilitate the administration of the Fund and as necessary to provide coverage and services to all of the Fund's participants. Health care operations includes: making eligibility determinations; contacting health care providers; providing participants with information about health-related issues or treatment alternatives; developing clinical guidelines and protocols; conducting case management; medical review and care coordination; handling claim appeals; reviewing health information to improve health or reduce health care costs; participating in drug or disease management activities; conducting

underwriting; premium rating or related functions to create, renew or replace health insurance or health benefits; and performing the general administrative activities of the Fund (such as providing customer service, conducting compliance reviews and auditing, responding to legal matters and compliance inquiries, handling quality assessment and improvement activities, business planning and development including cost management and planning related analyses and formulary development, and accreditation, certification, licensing or credentialing activities). For example, the Fund may use your health information to conduct case management of ongoing care or to resolve a claim appeal you file.

If the Fund discloses protected health information for underwriting purposes, the Fund is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

D. For Disclosure to the Plan Trustees. The Fund may disclose your health information to the Board of Trustees (which is the plan sponsor), or any insurer or HMO with which the Fund contracts, and to necessary advisors which assist the Board of Trustees in performing plan administration functions, such as handling claim appeals. The Fund also may provide summary health information to the Board of Trustees so that it may solicit bids for services or evaluate its benefit plans. Summary health information is information that summarizes participants' claims information but from which names and other identifying information have been removed. The Fund may also disclose information about whether you are participating in the Fund or one of its available options.

E. For Disclosure to You or Your Personal Representative. When you request, the Fund is required to disclose to you or your personal representative your protected health information that contains medical records, billing records, and any other records used to make decisions regarding your health care benefits. Your personal representative is an individual designated by you in writing as your personal representative, attorney-in-fact. The Fund may request proof of this designation prior to the disclosure. Also, absent special circumstances, the Fund will send all mail from the Fund to the individual's address on file with the Fund Administration Office. You are responsible for ensuring that your address with the Fund Administration Office is current. Although mail is normally addressed to the individual to whom the mail pertains, the Fund cannot guarantee that other individuals with the same address will not intercept the mail. You have the right to request restrictions on where your mail is sent as set forth in the request restrictions section below.

F. Disclosure Where Required By Law. In addition, the Fund will disclose your health information where applicable law requires. This includes:

(1) <u>In Connection With Judicial and Administrative Proceedings</u>

The Fund will in response to an order from a court or administrative tribunal disclose protected health information in accordance with the express terms of such an order. The Fund may also disclose protected health information in response to a subpoena or other lawful process if the Fund receives satisfactory documentation that you have received notice of the subpoena or legal process, the notice provided sufficient information to allow you to raise an objection and the time for raising an objection has passed and either no objections were filed or were resolved by the court or

administrative tribunal. Alternatively, the party requesting disclosure may provide satisfactory documentation you have agreed to the disclosure or that it has obtained a qualified protective order which meets the requirements of the Privacy Rules and which allows for disclosure. For example, if the Fund receives a court order requiring it to disclose certain information, it will respond to the court order.

(2) When Legally Required And For Law Enforcement Purposes

The Fund will disclose your protected health information when it is required to do so for law enforcement purposes. This may include compliance with laws which require reporting certain types of injuries, pursuant to court issued legal process; or a grand jury subpoena or other administrative requests if satisfactory documentation is provided that the request is relevant to a legitimate law enforcement purpose, the request is reasonably tailored to meet this legitimate law enforcement purpose and de-identified individual cannot be reasonably provided as an alternative. Additionally, limited disclosure may be made for purposes of identifying or locating a suspect, fugitive, material witness or missing person, identifying a victim of a crime or in connection with a criminal investigation that occurred on Fund premises. For example, the Fund could upon request of a law enforcement agency provide information concerning the address of a fugitive.

(3) To Conduct Public Health and Health Oversight Activities

The Fund may disclose your health information to a health oversight agency for authorized activities (including audits, civil administrative or criminal investigations, inspections, licensure or disciplinary action), government benefit programs for which health information is relevant, or to government agencies authorized by law to receive reports of abuse, neglect or domestic violence as required by law. The Fund, however, may not disclose your health information if you are the subject of an investigation and the investigation does not arise out of or is not directly related to your receipt of health care or public benefits.

(4) In the Event of a Serious Threat to Health or Safety

The Fund may, consistent with applicable law and ethical standards of conduct, disclose your health information if the Fund, in good faith, believes that such disclosure is necessary to prevent or lessen a serious and imminent threat to your health or safety or to the health and safety of the public. For example, the Fund may disclose evidence of a threat to harm another person to the appropriate authority.

(5) For Specified Government Functions

In certain circumstances, federal regulations require the Fund to use or disclose your health information to facilitate specified government functions related to the military and veterans, national security and intelligence activities, protective services for the president and others, and correctional institutions and inmates.

(6) For Workers Compensation

The Fund may release your health information to the extent necessary to comply with laws related to workers compensation or similar programs.

II. Authorization to Use or Disclose Health Information

Other than as stated above, the Fund will not disclose your health information without your written authorization. Generally, you will need to submit an Authorization if you wish the Fund to disclose your health information to someone other than yourself. Authorization forms are available from the Privacy Contact Person listed below. If you have authorized the Fund to use or disclose your health information, you may revoke that Authorization in writing at any time. The revocation should be in writing, include a copy of or reference to your Authorization and be sent to the Privacy Contact Person listed below.

Special rules apply about disclosure of psychotherapy notes. Your written Authorization generally will be required before the Fund will use or disclose psychotherapy notes. Psychotherapy notes are a mental health professional's separately filed notes which document or analyze the contents of a counseling session. They do not include summary information about your mental health treatment or information about medications, session stop and start times, the diagnosis and other basic information. The Fund may use and disclose psychotherapy notes when needed to defend against litigation filed by you or in other limited situations.

Your written authorization will be required for any disclosure of your health information that involves marketing, the sale of your health information, or any disclosure involving direct or indirect remuneration to the Fund.

III. Your Rights With Respect To Your Health Information

You have the following rights regarding your health information that the Fund maintains:

A. Right to Request Restrictions. You may request restrictions on certain uses and disclosures of your health information. You have the right to request a limit on the Fund's disclosure of your health information to someone involved in payment for your care. The Fund is not required to agree to your request unless the protected health information pertains solely to a health care item or service for which you, or a person on your behalf, has paid the provider or Plan in full, and the disclosure at issue is for the purpose of carrying out payment or health care operations .

B. Right to Inspect and Copy Your Health Information. You have the right to inspect and copy your health information. This right, however, does not extend to psychotherapy notes or information compiled for civil, criminal or administrative proceeding. The Fund may deny your request in certain situations subject to your right to request review of the denial. A request to inspect and copy records containing your health information must be made in writing to the Privacy Contact Person listed below. If you request a copy of your health information, the Fund may charge a reasonable fee for copying, assembling costs and postage, if applicable, associated with your request. Notwithstanding the foregoing, the fee for

a copy of your health information in electronic form shall not be greater than the labor costs in responding to the request.

C. Right to Receive Confidential Communications. You have the right to request that the Fund communicate with you in a certain way if you feel the disclosure of your health information through regular procedures could endanger you. For example, you may ask that the Fund only communicate with you at a certain telephone number or by e-mail. If you wish to receive confidential communications, please make your request in writing to the Privacy Contact Person listed below. The Fund will attempt to honor reasonable requests for confidential communications.

D. Right to Amend Your Health Information. If you believe that your health information records are inaccurate or incomplete, you may request that the Fund amend the records. That request may be made as long as the information is maintained by the Fund. A request for an amendment of records must be made in writing to the Fund's Privacy Contact Person listed above. The Fund may deny the request if it does not include a reasonable reason to support the amendment. The request also may be denied if your health information records were not created by the Fund, if the health information you are requesting to amend is not part of the Fund's records, if the health information you wish to amend falls within an exception to the health information you are permitted to inspect and copy, or if the Fund determines the records containing your health information are accurate and complete.

E. Right to an Accounting. You have the right to request a list of disclosures of your health information made by the Fund. The request must be made in writing to the Privacy Contact Person. The request should specify the time period for which you are requesting the information. No accounting will be given of disclosures made: to you; for Treatment, Payment or Health Care Operations; disclosures made before April 14, 2003 ; disclosures for periods of time going back more than six years ; pursuant to an authorization; or in other limited situations. The Fund will provide the first accounting you request during any 12-month period without charge. Subsequent accounting requests may be subject to a reasonable cost-based fee. The Fund will inform you in advance of the fee, if applicable.

F. Right to Opt Out of Fundraising Communications. In the event that the Fund engages in a fundraising activity, you have the right to opt out of any fundraising communications.

G. Right to a Paper Copy of this Notice. You have a right to request and receive a paper copy of this Notice at any time, even if you have received this Notice previously or agreed to receive the Notice electronically. To obtain a paper copy, please contact the individual listed below. If this Notice is modified, you will be mailed a new copy.

H. Privacy Contact Person/Privacy Official. To exercise any of these rights related to your health information you should contact :

Privacy Contact Person	Privacy Official
Robert Garcia Alaska Electrical Health & Welfare Fund 701 East Tudor, Suite 200 Anchorage, AK 99503 Telephone: (907) 276-1246 Toll Free: (800) 478-1246 E-mail: Robert_g@Aetf.com	Patti Janusiewicz Alaska Electrical Health & Welfare Fund 701 East Tudor, Suite 200 Anchorage, AK 99503 Telephone: (907) 276-1246 Toll Free: (800) 478-1246 E-mail: patti_j@Aetf.com

IV. Duties of the Fund

The Fund is required by law to maintain the privacy of your health information as set forth in this Notice, to provide to you this Notice summarizing its privacy practices and duties, and to notify you following a breach of unsecured protected health information. The Fund is required to abide by the terms of this Notice, which may be amended from time to time. The Fund reserves the right to change the terms of this Notice and to make the new Notice provisions effective for all health information that it maintains. If the Fund changes its policies and procedures, the Fund will revise the Notice and will provide you a copy of the revised Notice within 60 days of the change. You have the right to request a written copy of the Notice at any time.

You have the right to express complaints to the Fund and to the Secretary of the Department of Health and Human Services if you believe that your privacy rights have been violated. Any complaints to the Fund should be made in writing to the Privacy Official identified above. The Fund encourages you to express any concerns you may have regarding the privacy of your health information. You will not be retaliated against in any way for inquiring about or filing a complaint about privacy matters.

EFFECTIVE DATE

This Notice is effective **April 14, 2003 as amended September 23, 2013 and _____, 2025**.

Appendix B

ALASKA ELECTRICAL HEALTH AND WELFARE FUND

AUTHORIZATION FOR USE OR DISCLOSURE OF HEALTH INFORMATION

PERSON WHOSE PROTECTED HEALTH INFORMATION WILL BE DISCLOSED

Name:_____ Birth Date: _____/_____/____
MM DD YR

Address:
_____
_____
_____

Home Telephone No.:

Work Telephone No.:

E-mail Address:
_____

Last 4 digits of the Covered Employee's Social Security Number:
_____

PURPOSE OF AUTHORIZATION

This Authorization is required for the Fund to release your health information to someone other than yourself or for purposes outside the Fund's normal operations (treatment, payment of claims or healthcare operations). The recipients of this Authorization will rely on it to disclose your health information. Please review it carefully.

NATURE OF DISCLOSURE BEING AUTHORIZED

The information requested in Questions 1 through 7 must be provided for this Authorization to be effective.

1. **Describe Information To Be Disclosed**: Identify here what you authorize to be used or disclosed. The information should be specific such as "Information related to my knee surgery":

List information here: _____
_____

2. **Describe the Purpose of the Disclosure**: List why the information is being disclosed. If you are initiating the request, you can simply check here: ☐ At the request of the individual. Otherwise, list the purpose:

_____
_____

3. **Identify Who Is Authorized to Disclose the Information:** Identify here who is authorized to make the disclosure.

   ☐ **All entities with information about the matters listed in paragraph 1**
   ☐ Only the following entities: _____
   _____

4. **Identify Who Will Receive the Information:** List here who is authorized to receive information such as "Mary Jones, my spouse" or "John Doe, my union representative."

   _____
   _____

5. **Identify How To Provide Information:** Where and how should the information be disclosed? List address, e-mail, facsimile, etc. Please remember that the information being sent is your private health information.

   _____
   _____

6. **Expiration Date of Authorization:** Indicate when your authorization will end. This can be a date ("December 31, 2018") or the happening of an event ("when my appeal is resolved"). Unless otherwise indicated this authorization will be good for one year.

   a. ☐ For one year from the date of the authorization
   b. ☐ Until _____/_____/_____
      MM DD YR
   c. ☐ Upon the occurrence of the following event: _____
      _____

7. **Signature and Date: Important – This document must be signed and dated.**

   Signature and Date: _____

STATEMENT OF RIGHTS REGARDING THIS AUTHORIZATION

General Rights. I understand I am not required to sign this form and that a Covered Entity receiving it cannot condition treatment, payment or eligibility on my decision to sign this form. I understand, however, that a health plan can condition enrollment in the Plan or eligibility for benefits on receiving an authorization if the purpose is to allow the health plan to obtain information it needs to make an eligibility, enrollment or underwriting decision and psychotherapy notes are not requested.

Right to Revoke. I understand that I have the right to revoke this authorization in writing except as to uses and/or disclosures already made in reliance on it. Authorization revocation forms can be obtained by contacting the Privacy Contact Person listed in the Fund's Privacy Notice.

Effect of Disclosure. I understand that if the persons to whom my health information is disclosed are not subject to the HIPAA Privacy Rule (i.e. are not a health plan, health care provider or health

care clearinghouse), the disclosed health information may no longer be protected by the HIPAA Privacy Rule and may be redisclosed without my authorization.

Retention and Right to Copy. I understand that the Fund must retain a copy of this Authorization and provide me a copy.

Provisions Related to Psychotherapy Notes. I understand that an Authorization is required for any use or disclosure of psychotherapy notes as defined in 45 CFR 164.508(a)(2) except in the limited situations dealing with treatment, training or defense of legal actions.

PERSONAL REPRESENTATIVE

This section only needs to be answered if this authorization is being completed by someone other than the individual to whom the health information relates.

If this Authorization is being completed by someone as a personal representative of the individual to whom the health information relates, this section must be completed and signed.

The Fund, for purposes of the Privacy Rule will treat a properly designated personal representative as the individual for purposes of the Privacy Rule. This will apply when the individual is deceased, the personal representative has been designated in accordance with applicable law, or in the case of unemancipated minors, an authorization is required as a result of state law. The Fund reserves the right to decline to recognize an individual as a personal representative if there is a reasonable belief that the individual whose information would be disclosed has been or could be subject to abuse, neglect or endangerment by disclosure. Disclosure also will not be made if inconsistent with applicable law.

Except as limited by state law or the Privacy Rules, no authorization is needed to disclose information to a natural parent or legal guardian of an unemancipated minor. A statement concerning disclosure of information regarding minors is available from the Contact Person listed in the Fund's Privacy Notice.

a. Name of Personal Representative: _____

b. Basis for Being Personal Representative (e.g. guardian, executed health care power of attorney, etc.) Identify basis or attach a copy of any document creating your authority to act for the named individual. _____
_____
_____

Address: _____ Telephone No.: _____
_____ E-mail Address: _____
_____

Signature: _____ Date: _____

Appendix C

MODEL BUSINESS ASSOCIATE AGREEMENT
between
ALASKA ELECTRICAL HEALTH AND WELFARE TRUST
and
[NAME OF BUSINESS ASSOCIATE]

This Business Associate Agreement ("Agreement") is between the **ALASKA ELECTRICAL HEALTH & WELFARE TRUST** ("Trust") and **[NAME OF BUSINESS ASSOCIATE]** ("Business Associate") (collectively the "Parties") to be effective _____. This Agreement supplements the contract for services between the Trust and Business Associate that is currently in effect or as may be amended, supplemented, or extended from time to time (the "Contract").

The Trust and Business Associate agree to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Subtitle D of the American Recovery and Reinvestment Act of 2009 ("HITECH"), as set forth in Title 45, Parts 160, 162, and 164 and Title 42, Part 1320d of the Code of Federal Regulations (the "CFR"). In the event of conflicting terms or conditions between this Agreement and the Contract, the terms of this Agreement shall supersede the conflicting terms of the Contract and any prior business association agreement between the Parties

A. Definitions. Capitalized terms not otherwise defined in this Agreement shall have the meanings given to them in 45 CFR Parts 160, 162, and 164 and are incorporated herein by reference.

B. Use and Disclosure of Protected Health Information. Business Associate shall use and/or disclose Protected Health Information ("PHI") only if such use and/or disclosure is in compliance with each applicable requirement of 45 CFR 164.502(a) and § 164.504(e) and is necessary to satisfy Business Associate's obligations under this Agreement and the Contract. The Parties acknowledge that the privacy rules referenced in 45 CFR § 164.504(e) shall apply to the Business Associate in the same manner as such rules apply to the Trust.

C. Prohibition on Unauthorized Use or Disclosure of PHI. Business Associate shall not use or disclose any PHI received from or on behalf of the Trust except as permitted or required by this Agreement, as required by law, or as otherwise authorized in writing by the Trust. Business Associate shall comply with: (a) 45 CFR Part 164; and (b) state laws, rules, and regulations applicable to PHI not preempted pursuant to 45 CFR Subpart B of Part 160 or the Employee Retirement Income Security Act of 1974 ("ERISA") as amended.

D. Business Associate's Operations. Business Associate may use PHI it creates or receives for or from the Trust only to the extent necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities. Business Associate may disclose such PHI as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities only if:

(i) The disclosure is required by law; or

(ii) Business Associate obtains reasonable assurance, evidenced by written contract from any person or organization to which Business Associate discloses such PHI, that such person or organization shall:

(i) Agree to the same restrictions and conditions that apply to the Business Associate with respect to such information;

(ii) Hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it or as required by law; and

(iii) Notify Business Associate (who shall in turn promptly notify the Trust) of any instance in which the confidentiality of such PHI was breached.

E. Data Aggregation Services. Business Associate may use PHI to provide Data Aggregation Services related to the Trust's Health Care Operations as permitted by 45 CFR § 164.504(e)(2)(i)(B).

F. De-Identification of PHI. Business Associate may de-identify PHI in the course of providing services to the Trust.

G. PHI Safeguards. Business Associate shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to prevent the improper use or disclosure of any PHI received from or on behalf of the Trust.

H. Minimum Necessary. When using, disclosing, or requesting PHI to and from the Trust, the Trust's other business associates, or Business Associates' subcontractors or agents, the Parties shall limit PHI, to the extent practicable, to a Limited Data Set as defined by 45 CFR § 164.514(e)(2) or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request in accordance with guidance provided by the Secretary of the Department of Health and Human Services. The Parties acknowledge that each may rely on the other's determination of the minimum necessary for compliance with the minimum necessary standards. The Parties will ensure that any agents agree to the same restrictions and conditions that apply to the Limited Data Set.

I. Electronic Health Records Security and Integrity. The Business Associate and the Trust acknowledge that Title 42, Section 1320d-2(d) of the United States Code and 45 CFR Part 164.302, *et seq.* apply to the Business Associate in the same manner as such sections apply to the Trust. The Business Associate shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards in compliance with Title 42, Section 1320d-2(d) of the United States Code and 45 CFR Part 164.302, *et seq*. that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Health Records that the Business Associate creates, receives, maintains, or transmits on behalf of the Trust. Business Associate shall document and keep these security measures current. Business Associate in deciding which security measures to use will take into account the following:

(i) The size, complexity and capabilities of the Business Associate, and

(ii) The technical infrastructure, hardware, and software security capabilities.

Business Associate agrees to adopt required implementation specifications, review and modify security measures as needed to continue to provide reasonable and appropriate

protection of electronic PHI, assess whether optional implementation specifications are reasonable and appropriate safeguards of PHI, and update documentation of each security measure.

Business Associate shall also ensure that any of its agents and subcontractors, to whom it provides such information, agree to implement reasonable and appropriate security measures. Business Associate agrees to document the satisfactory assurances received from its agents and subcontractors.

Business Associate shall report to the Trust any "Security Incident," as defined in 45 CFR § 164.304, of which it becomes aware. The report will be made in accordance with the reporting procedures in Section 17 of this Agreement. Business Associate agrees to identify and respond to suspected or known Security Incidents; mitigate harmful effects of Security Incidents, to the extent practicable; and document Security Incidents and their outcomes.

J. Protection of Exchanged Information in Electronic Transactions. If Business Associate conducts any Standard Transaction for or on behalf of the Trust, Business Associate shall comply with each applicable requirement of 45 CFR Part 162. Business Associate shall not enter into any Trading Partner Agreement in connection with the conduct of Standard Transactions for or on behalf of the Trust that: (a) changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard; (b) adds any Health Information elements or segments to the maximum defined Health Information set; (c) uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification or are not in the Standard's Implementation Specification(s); or (d) changes the meaning or intent of the Standard's Implementation Specification(s).

K. Subcontractors and Agents. Business Associate shall require each of its subcontractors or agents that create, receive, maintain, or transmit PHI on behalf of the Trust to agree to written contractual provisions that impose the same obligations to protect such PHI as are imposed on Business Associate by this Agreement.

L. Access to PHI. At the request of the Trust, Business Associate shall provide to the Trust access to PHI in a Designated Record Set; or, as directed by the Trust, to an Individual to meet the requirements under 45 CFR § 164.524 and applicable state law. Business Associate shall provide access in the time and manner set forth in the Trust's Privacy Policy and Procedures.

M. Amending PHI. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that the Trust directs or agrees to pursuant to 45 CFR § 164.526 at the request of the Trust or an Individual, and in the time and manner set forth in the Trust's Privacy Policy and Procedures.

N. Accounting of Disclosures of PHI.

(i) Business Associate shall document such disclosures of PHI and Electronic Health Records and information related to such disclosures as would be required for the Trust to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

(ii) Business Associate agrees to provide the Trust, or at the Trust's direction, an Individual, information collected in accordance with section (a) above, to permit the Trust to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

O. Sales of PHI and Marketing. The Business Associate agrees that it shall not engage in the sale of PHI and shall not directly or indirectly receive remuneration in exchange for PHI unless expressly permitted by the Contract and applicable law.

P. Access to Books and Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or on behalf of the Trust available to the Trust and to DHHS or its designee for the purpose of determining the Trust's compliance with HIPAA. Business Associate shall notify the Trust in writing within 10 days of any request by DHHS for information relating to the Trust, and upon request from the Trust provide the Trust a copy of any such information that is provided to DHHS.

Q. Reporting. If the Business Associate becomes aware of or receives a written complaint of any use, unauthorized disclosure, or Breach of PHI, it shall submit a written report of the complaint or incident to the Trust's Privacy Official not less than ten business days after Business Associate's receipt of the complaint or discovery of the Breach. Business Associate's report shall at least: (i) identify the nature of the unauthorized use or disclosure; (ii) identify each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed; (iii) identify the PHI used or disclosed including the types of identifiers and the likelihood of re-identification; (iv) identify who made the unauthorized use or received the unauthorized disclosure; (v) identify whether the PHI was actually acquired or viewed; (vi) identify what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; (vii) identify what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure; and (viii) provide such other information, including a written report, as reasonably requested by the Trust's Privacy Official. Business Associate shall cooperate with the Trust in providing any notice to affected Individuals, local media, and governmental agencies as required by law.

Business Associate also agrees to report all information necessary about any breaches of PHI in order for the Trust to include such information in the Trust's log of Breaches filed annually, as necessary, with DHHS.

Business Associate agrees to cooperate with the Trust in preparing and sending Breach notifications and shall pay the costs of such notifications for Breaches associated with PHI held by Business Associate or its agents or subcontractors.

R. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

S. Business Associate Not an Agent. The Parties agree that Business Associate is not acting as an agent of the Trust under either this Agreement or the Contract.

T. Penalties for Noncompliance. Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with HIPAA, to the extent provided by HITECH and the HIPAA privacy rules.

U. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Trust to comply with applicable law.

V. Obligations of the Trust.

(a). Provisions for the Trust to Inform the Business Associate of Privacy Practices and Restrictions.

(i.) The Trust shall notify the Business Associate of any limitation(s) in the notice of privacy practices of the Trust in accordance with 45 CFR §164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of Protected Health Information.

(ii.) The Trust shall notify the Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect the Business Associate's use or disclosure of Protected Health Information.

(iii.) The Trust shall consult with the Business Associate as to the administrative practicality of a restriction prior to agreeing to a restriction that affects the Business Associate's use or disclosure of Protected Health Information. The Trust shall also notify the Business Associate of any restriction to the use or disclosure of Protected Health Information that the Trust has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of Protected Health Information.

(iv.) The Trust shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Trust, except as otherwise contemplated herein.

W. Termination.

(i) Upon either Party's knowledge of a material breach of this Agreement by the other Party or its subcontractors or agents, the non-breaching Party shall provide an opportunity for breaching Party to cure the breach or end the violation. If the breaching Party or its subcontractors or agents do not cure the breach or end the violation within the time specified by the non-breaching Party, or if cure is not possible, the non-breaching Party shall have the right to terminate this Agreement and the Contract.

(ii) Notwithstanding any other provision of this Agreement or the Contract, either Party shall have the right to terminate this Agreement and the Contract if it determines, in its sole discretion, that the other Party or its subcontractor or agents has violated a material term of this Agreement related to the use or disclosure of PHI or any

provision of 45 CFR Parts 160, 162 and 164. This right may be exercised by providing written notice to the other Party of termination, with such notice stating the violation that provides the basis for the termination. Any such termination shall be effective immediately or at such other date specified in such notice.

(iii) This Agreement shall also automatically terminate at the later of the termination of the Contract, or a successor agreement to the Contract.

(iv) This Agreement may be terminated by mutual written agreement of the Parties.

X. Return or Destruction of PHI.

(i) Except as provided in section (b) below, upon termination Business Associate shall return to the Trust or destroy all PHI received from the Trust or created or received by Business Associate on behalf of the Trust. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. Business Associate shall complete such return or destruction as promptly as possible, but not later than 30 days after the effective date of the termination of the Contract. Business Associate shall retain no copies of the PHI.

(ii) In the event that Business Associate determines that returning or destroying the PHI is infeasible due to the records retention requirements of ERISA, the AICPA (if applicable), or other similar law or guidance, Business Associate shall provide within 30 days of the effective date of termination written justification explaining why such PHI could not be returned or destroyed. Upon verification by the Trust that the return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further use and disclosure of PHI to those purposes that make the return or destruction infeasible for so long as Business Associate maintains such PHI. Reference to the destruction of PHI in this paragraph shall be interpreted in accordance with the record retention requirements of ERISA, the AICPA (if applicable), and 45 CFR §164.530(j)(2).

Y. Survival. Business Associate's obligation to protect PHI and Health Information received from or on behalf of the Trust shall be continuous and shall survive any termination of this Agreement and the Contract.

Z. Indemnification. Business Associate agrees to indemnify the Trust against all civil penalties imposed by DHHS for all acts or omissions which violate an administrative simplification provision, as defined by 45 CFR § 160.103, performed by Business Associate or Business Associate's subcontractor.

For all other claims and causes of action, each party shall indemnify and hold harmless the other from and against any claim, cause of action, liability, damage, cost, or expense (including reasonable attorney fees) arising out of its unauthorized use or disclosure of PHI or other breach of this Agreement.

This Section shall survive termination of this Agreement.

AA. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with the Health Insurance Portability and Accountability Act of 1996 and Subtitle D of the American Recovery and Reinvestment Act of 2009, as set

forth in Title 45, Parts 160, 162 and, 164 and Title 42, Part 1320d of the Code of Federal Regulations.

BB. Governing Law. The laws of the state of Alaska apply to this Agreement to the extent not preempted by 45 CFR Subpart B of Part 160 or the Employee Retirement Income Security Act of 1974 as amended.

Appendix D

Summary of Alaska State Laws Governing Disclosure of a Minor's PHI

The law of the state where the minor resides will control what PHI may be disclosed to a parent or legal guardian. Disclosure issues involving minors living in states other than the State of Alaska will be referred to Trust Legal Counsel.

Alaska. Alaska law limits disclosure of an unemancipated minor's PHI without an authorization in the following situations:

(1) A minor may give consent for medical and dental services if the parent or legal guardian of the minor cannot be contacted or, if contacted, is unwilling either to grant or withhold consent; however, where the parent or legal guardian cannot be contacted or, if contacted, is unwilling either to grant or to withhold consent, the provider of medical or dental services shall counsel the minor keeping in mind not only the valid interests of the minor but also the valid interests of the parent or guardian and the family unit as best the provider presumes them.

(2) A minor who is the parent of a child may give consent to medical and dental services for the minor or the child.

(3) A minor may give consent for diagnosis, prevention or treatment of pregnancy, and for diagnosis and treatment of venereal disease.