HIPAA

PRIVACY POLICIES AND PROCEDURES

FOR

TONGASS TIMBER TRUST

October 2004
Effective April 13, 2004

TABLE OF CONTENTS

1. MINIMUM NECESSARY 1
   1.1 POLICY STATEMENT 1
2. USE OF AUTHORIZATIONS 3
   2.1 POLICY STATEMENT 3
   2.2 PROCEDURES 3
   AUTHORIZATION FORM 5
3. DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR PUBUC HEALTH, LAW ENFORCEMENT, OR LEGAL PROCESS 7
   3.1 POLICY STATEMENT 7
   REQUEST FOR ACCESS TO PHI WITHOUT AUTHORIZATION FROM INDIVIDUAL FORM 13
4. CERTIFICATION & PLAN DOCUMENT AMENDMENT 14
   4.1 POLICY STATEMENT 14
   SAMPLE CERTIFICATION TO GROUP HEALTH PLAN, HMO OR HEALTH INSURANCE ISSUER 16
   USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION 18
5. DE-IDENTIFICATION 21
   5.1 POLICY STATEMENT 21
6. VERIFICATION 23
   6.1 POLICY STATEMENT 23
7. RECOGNITION OF PERSONAL REPRESENTATIVE 29
   7.1 POLICY STATEMENT 29
   7.2 PROCEDURES 30
   APPOINTMENT OF PERSONAL REPRESENTATIVE FORM 31
8. USE & DISCLOSURE FOR INVOLVEMENT IN AN INDIVIDUAL'S CARE OR PAYMENT 33
FOR CARE AND FOR NOTIFICATION PURPOSES 33
   8.1 POLICY STATEMENT 33
9. CLAIMS AND APPEALS 35
   9.1 PRIVACY POLICY STATEMENT 35
   9.2 PRIVACY PROCEDURES 35
10. RIGHT TO REQUEST RESTRICTIONS ON USE & DISCLOSURE 36
   10.1 POLICY STATEMENT 36
   10.2 PROCEDURES 36
   PRIVACY PROTECTION REQUEST FORMS 38
   REQUEST FOR RESTRICTIONS ON USE & DISCLOSURE FORM 39
   DENIAL OF REQUEST FOR RESTRICTION ON USE & DISCLOSURE FORM 40
11. RIGHT TO REQUEST INFORMATION BE TRANSMITTED BY ALTERNATIVE MEANS 41
   11.1 POLICY STATEMENT 41
   11.2 PROCEDURES 41
   REQUEST FOR INFORMATION BE TRANSMITTED BY ALTERNATIVE MEANS FORMS 42
   REQUEST THAT PHI BE TRANSMITTED BY ALTERNATIVE MEANS FORM 43
   DENIAL OF REQUEST FORM THAT PHI BE TRANSMITTED BY ALTERNATIVE MEANS FORM 44
12. RIGHT OF ACCESS TO PHI 45
   12.1 POLICY STATEMENT 45
   12.2 PROCEDURES 45
   RIGHT OF ACCESS TO PHI FORMS 48
   REQUEST FOR ACCESS TO PHI FORM 49
   NOTICE OF EXTENSION OF TIME TO DECIDE REQUEST FOR ACCESS TO PHI 50
   DENIAL OF REQUEST FOR ACCESS TO PHI FORM 51
13. RIGHT TO AMEND PHI 52
   13.1 POLICY STATEMENT 52
   13.2 PROCEDURES 52
   RIGHT TO AMEND PHI FORMS 55
   REQUEST TO AMEND PHI FORM 56
   DENIAL OF REQUEST TO AMEND PHI FORM 57
   STATEMENT DISAGREEING WITH DENIAL OF REQUEST TO AMEND PHI 58

REBUTTAL TO STATEMENT DISAGREEING WITH DENIAL OF REQUEST TO AMEND PHI 59
ACCEPTANCE OF REQUEST TO AMEND PHI FORM 60
14. RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI 61
14.1 POLICY STATEMENT 61
14.2 PROCEDURES 61
REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORMS 64
DENIAL OF REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM 64
REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM 65
ACCOUNTING FOR DISCLOSURES OF PHI FORM 66
DENIAL OF REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM 68
15. DISTRIBUTION OF PRIVACY NOTICE 69
15.1 POLICY STATEMENT 69
15.2 PROCEDURES 69
NOTICE OF PRIVACY PRACTICES 70
16. TRAINING 75
16.1 POLICY STATEMENT 75
16.2 PROCEDURES 75
17. COMPLAINTS FOR VIOLATION OF PRIVACY RULES 76
17.1 POLICY STATEMENT 76
17.2 PROCEDURES 76
COMPLAINT FORM 78
REPORT OF COMPLAINT INVESTIGATION FORM 79
18. ANTI-RETALIATION 80
18.1 POLICY STATEMENT 80
19. MITIGATION OF HARMFUL EFFECTS 81
19.1 POLICY STATEMENT 81
20. SANCTIONS FOR VIOLATION OF PRIVACY RULES 82
20.1 POLICY STATEMENT 82
20.2 PROCEDURES 82
REPORT OF PRIVACY RULES VIOLATION FORM 84
SANCTION FOR VIOLATION OF PRIVACY RULES FORM 85
21. JOB DESCRIPTION FOR PRIVACY OFFICER 86
22. MARKETING 88
22.1 POLICY STATEMENT & PROCEDURE 88
23. RECORD RETENTION 89
23.1 POLICY STATEMENT 89
RECORD RETENTION POLICY 89
23.2 PROCEDURES 90
24. ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS 93
24.1 POLICY STATEMENT 93
24.2 PROCEDURES 93

1. MINIMUM NECESSARY

1.1 POLICY STATEMENT

This policy and procedure is adopted by the Trustees of the Tongass Timber Trust (the “Trust”) pursuant to Section 164.502(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

MINIMUM NECESSARY POLICY

The HIPAA Privacy Rules require that when using or disclosing Protected Health Information ("PHI"), or when requesting PHI from another covered entity, the Trust will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Trust must implement policies and procedures for routine uses and disclosures. As long as policies and procedures exist, The Trust does not need to make individual assessments of each routine use or disclosure.

THE TRUST MUST IDENTIFY:

- The persons or classes of persons, as appropriate, in the workforce who need to access PHI to carry out their duties, and

- For each person or class of persons: (a) the category of PHI to which access is needed; and (b) any conditions appropriate to such access. 45 CFR 164.514(d).

1. The Trust will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose when (a) using PHI, (b) disclosing PHI, and (c) requesting PHI.

2. The minimum necessary standard applies to oral, electronic, and written PHI.

3. The Trust will identify the categories or types of PHI needed.

4. The Trust will identify the conditions appropriate to access to PHI.

ROUTINE DISCLOSURES

5. When information is disclosed to the Trustees, the insurer or the administrator will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose.

6. When receiving a request for PHI from one of the following categories of individuals, the Trust may rely on the judgment of the requestor as to the minimum amount of information that is necessary:

   a. A public officer or agency for a disclosure to them that is permitted under HIPAA
   b. A health plan, health care clearinghouse, or health care provider that is covered by the HIPAA rules
   c. A Business Associate

   The disclosure would be considered a routine disclosure and the Privacy Officer would not have to review it. However, if the request is vague or over-broad, the insurer or the administrator may seek clarification before responding.

   Business Associate Agreements should require a Business Associate to request from the Trust only the minimum information necessary to perform their functions on behalf of the Trust.

7. Routine disclosures to a Business Associate, as listed in this document, have been reviewed by the Trust and are consistent with the minimum necessary rule.

NON-ROUTINE DISCLOSURES

8. The Privacy Officer must approve any non-routine disclosures. A non-routine disclosure is a disclosure of PHI that is not addressed by the minimum necessary protocols. Each non-routine disclosure must be reviewed on an individual basis. The criteria for reviewing a non-routine disclosure are as follows:

    a. The non-routine disclosure must be necessary to allow the Trust to carry out its obligations under ERISA and the governing plan documents.

    b. The non-routine disclosure must be limited to the information reasonably necessary to accomplish the purpose of the disclosure.

    c. The non-routine disclosure must be otherwise consistent with the Trust's privacy policies.

    d. The non-routine disclosure must not be prohibited by the HIPAA privacy rules.

    e. A request for a non-routine disclosure that is accompanied by an individual written authorization that is compliant with HIPAA will be honored in a manner consistent with the Trust's privacy policies.

REQUESTS

9. When requesting PHI from another health plan the Trust will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose.

10. When requesting medical records from a health care provider, the Trust will not request the entire medical file, but only that portion necessary to accomplish the intended purpose. If the insurer or administrator determines that the entire medical file must be requested, the Privacy Officer must approve the request and authorization from the individual is required.

11. Neither the insurer nor the administrator will not request psychotherapy notes without written authorization from the individual. Psychotherapy notes are notes recorded in any medium by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session. Psychotherapy notes are only those notes that are kept separate from the rest of the medical record. Summary medical information regarding psychotherapy may be used without written authorization if for treatment, payment or health care operations purposes.

MINIMUM NECESSARY RULE NOT APPLICABLE

Pursuant to the HIPAA privacy rules, the minimum necessary principles do not apply to the following uses, disclosures and requests for PHI:

1. Disclosures or requests to a health care provider for treatment purposes.

2. Disclosures to the individual who is the subject of the PHI. Identity of the individual must be verified.

3. Disclosures based on an authorization.

4. Disclosures to U.S. Department of Health and Human Service for compliance and enforcement purposes related to HIPAA's administrative simplification requirements.

5. Uses or disclosures required by other laws.

6. Uses or disclosures required for compliance with HIPAA's electronic data interchange (EDI) transaction standards.

2. USE OF AUTHORIZATIONS

2.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.508 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

USE OF AUTHORIZATIONS PRIVACY POLICY

Except as otherwise provided under the privacy regulations or other applicable law, the Trust may not use or disclose PHI without a valid authorization. An authorization is not required for use or disclosure of PHI for treatment, payment or health care operations or for uses or disclosures otherwise permitted under the privacy rules.

If an authorization is asked for or received, the Trust will only use or disclose PHI in a manner consistent with the authorization.

2.2 PROCEDURES

1. A valid authorization is required for any use or disclosure of PHI, except as provided under these procedures or under the privacy regulations.

2. An authorization is not required for use or disclosure of PHI for treatment, payment or health care operations.

3. The Trust will seek authorization for the following uses of PHI:

    a. Use of health information to administer a claim for Life/AD&D benefits.

4. Unless otherwise provided for in the Trust's Privacy Policies and Procedures, the Trust will seek authorization for the following disclosures of PHI except when the disclosure is required for treatment, payment or healthcare operations:

    a. Disclosure to a third party, such as a an employer’s human resources staff, related to eligibility, claims, reports and other documents for benefits for an injury or illness, payment or lack of payment of benefits, appeal of an adverse benefit determination, workers' compensation and third party liability claims.

5. If the Trust seeks an authorization for a use or disclosure of PHI, the Trust must provide the Individual With a copy of the signed authorization.

6. The Privacy Officer or designee may make a determination as to whether a specific use or disclosure of PHI requires an authorization.

7. The Trust will obtain an authorization for the use or disclosure of psychotherapy notes except:

    a. Use or disclosure by the Trust to defend a legal action, or

    b. Use or disclosure to the Secretary 'of Health and Human Services (HHS) regarding compliance with HIPAA privacy rules,

    c. Use or disclosure as required by law,

    d. Use or disclosure for health oversight activities with respect to the oversight of the originator of the notes,

    e. Use or disclosure to coroners and medical examiners,

f. Use or disclosures to an individual, when requested under, and as required by their right to inspect, copy and receive an accounting of their PHI,

g. Use or disclosures, consistent with applicable law and standards of ethical conduct, where the insurer or the administrator in good faith believe the use or disclosure is necessary, to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is to a person reasonably able to prevent or lessen the threat, including the target of the threat.

8. The Trust will use authorizations for marketing purposes.

9. If the Privacy Officer or designee determines that an authorization is required, then the Trust will attempt to obtain a valid authorization from the individual.

10. The Privacy Officer will use the Trust's authorization form. Additional information may be included on the form as long as it is not inconsistent with the form.

11. When the form is sent back by the covered individual, the Privacy Officer will review the form to ensure that it is signed and complete. If the form has not been signed, is not properly completed or is otherwise defective, the Privacy Officer will re-send the form to the covered individual within ten business days with an explanation of the reason for rejecting the form.

12. The authorization must have an expiration date or event and must be signed and dated.

13. An authorization is not valid if:

    a. The expiration date has passed or the expiration event is known by the Privacy Officer to have occurred.
    b. The authorization has not been filled out completely.
    c. The authorization is known by the Privacy Officer to have been revoked.
    d. Any material information in the authorization is known by the Privacy Officer to be false.

14. Authorizations should be on separate forms. If two authorizations are required, separate forms should be used.

15. The Trust will generally not condition the provision to an individual of treatment, payment, enrollment or eligibility on receipt of an authorization from the individual. However, the Trust may condition enrollment in the plan or eligibility for benefits on receipt of authorization prior to enrollment, if the authorization is sought for underwriting or risk rating determinations and does not relate to psychotherapy notes.

16. If a personal representative signs the authorization form, then there must be proof of the representative's authority on file with the Privacy Officer.

17. An individual may revoke an authorization at any time by providing a signed written notice to the Privacy Officer by mail, facsimile or hand-delivery. An oral revocation will not be valid. A revocation will not be valid to the extent the Trust has relied on the authorization.

18. The Privacy Officer will retain all authorizations for at least six years from the expiration date of the authorization.

AUTHORIZATION FORM
FOR
USE AND DISCLOSURE OF HEALTH INFORMATION

Read this First!

1. **Do not use this Authorization Form for information on a claim for benefits. Submit an authorization form to your insurance company on its authorization form.**
2. **This Authorization Form is two pages. Complete both pages.**
3. **Return this Authorization Form to the address below.**

Section 1. Whose Health Information Will be Used or Disclosed Pursuant to this Authorization?

Name of Individual	Individual's Birth Date / /
The Individual named above is *(check one)*: ☐ The Employee who is covered by the health plan ☐ Spouse of the Employee who is covered by the health plan *(print Employee's name below)* ☐ Child of the employee who is covered by the health plan *(print Employee's name below)* Employee's name:	

Section 2. Who is Signing this Authorization?

☐ I am the Individual identified in Section 1.
☐ I am the personal representative of the individual identified in Section 1. I am *(print your name):* _____ I have the authority to sign on behalf of the Individual because I am *(check one)*: ☐ the parent of the Individual ☐ the legal guardian of the Individual ☐ the holder of a power of attorney that grants me authority to act on behalf of the Individual in making decisions related to his or her health care *If you are the legal guardian or holder of a power of attorney, submit the legal document that makes you legal guardian or submit the power of attorney.*

Section 4. Mailing Address and Telephone Number of Person Signing this Authorization

Mailing Address	Telephone Number

Section 5. Authorization

I authorize the Tongass Timber Trust and its business associates to use and disclose the health information of the Individual named in Section 1 above as described in the Sections below.

Section 6. Health Information to be Disclosed (*Check all that apply*)

☐ Individual's Coverage Information ☐ Individual's Eligibility Date (Coverage Date) ☐ Employee's Hire Date* ☐ Date Employee entered Eligible Class* *Must be authorized by Employee	☐ Individual's Address and Phone Number ☐ Individual's Birth Date ☐ Individual's Gender ☐ Individual's Prior Coverage
☐ Other *(describe)*	
☐ Exclude the following information *(describe)*	

Section 7. Persons/Organizations Authorized to Receive the Individual's Health Information

Name	Telephone Number
Address	

Section 8. Purpose or Need for the Disclosure ***(check one)***

☐ At the request of the Individual (or parent, guardian or holder of power of attorney named in Section 2 above)
☐ Other *(describe)*

Section 9. Expiration Date

This Authorization expires: *(check one)*

☐ Upon completion of the requested disclosure	☐ On *(enter date)* / /
☐ When the following event occurs *(describe)*	☐ Other *(describe)*
If no box is checked and completed, this Authorization expires 60 days from the date I sign this Authorization.	

Section 10. Important Information About Your Rights

I understand:

- I may refuse to sign this Authorization. This Authorization is voluntary.
- I may revoke this Authorization at any time before its expiration date by notifying the Tongass Timber Trust in writing.
- My revocation of this Authorization will not have any affect on use or disclosure of my health information before the Tongass Timber Trust received my revocation.
- I may see and copy the information described on this form if I ask for it.
- I am not required to sign this form to receive my health care benefits (enrollment, treatment, or payment).
- The person or organization who receives the information that is used or disclosed pursuant to this Authorization may redisclose it, unless that person or organization is a health plan, health care provider or health care clearinghouse that is subject to Federal healthcare privacy laws. If the information is redisclosed it may not be subject to Federal healthcare privacy laws. I have the right to seek assurances from that person or organization that he, she or it will not redisclose the information to any other party without my further authorization.

Section 11. Signature and Date

Signature of Individual or Representative	Date

Section 12. Authority Documentation (Guardian or Holder of Power of Attorney)

If you are the Individual's guardian or holder of a power of attorney for the Individual, check which document you are submitting with this Authorization *(check one)*: ☐ Legal document making me the Individual's guardian ☐ Power of attorney granting me authority to act on behalf of the Individual in making decisions related to health care

Return this Authorization to:
Tongass Timber Trust
Privacy Officer
111 Stedman, Suite 200
Ketchikan, AK 99901
Phone: 907-225-6114

For internal use. Received by:	Date received

3. DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR PUBUC HEALTH, LAW ENFORCEMENT, OR LEGAL PROCESS

3.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.512 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

DISCLOSURE OF PHI FOR PUBLIC HEALTH, LAW ENFORCEMENT, OR LEGAL PROCESS POLICY

The Trust may use and disclose Protected Health Information (PHI) for Public Health, Law Enforcement, or Legal Process purposes under the following conditions:

- The Trust may disclose this information without the consent or authorization of the individual who is the subject of the information.
- The Trust is not required to give the individual the opportunity to agree or object to the use or disclosure.
- These uses and disclosures must comply with the minimum necessary rule - that is the information used or disclosed must be limited to that minimally necessary to accomplish the business purpose. (Only uses and disclosures required by court order are not subject to the minimum necessary rule.)
- In all cases involving these uses and disclosures, the Privacy Officer or his or her designee must review and authorize the use or disclosure.
- Verification of the identity of public officers requesting PHI should be made pursuant to the Trust's Verification Policies and Procedures.
- The uses and disclosures listed below are permitted by the HIPAA privacy rules, but the Trust reserves the right to refuse to make the disclosure or to seek legal guidance regarding whether the disclosure should be made, including but not limited to seeking guidance from a court of applicable jurisdiction.

1. USES AND DISCLOSURES REQUIRED BY LAW

The Trust may use or disclose PHI to the extent that the use or disclosure is required by law. The use or disclosure must comply with and be limited to the relevant requirements of the law. If the use or disclosure is to report abusive situations, to comply with judicial or administrative legal process, or for law enforcement purposes, the use or disclosure must also comply with these policies and procedures.

Uses and disclosures that are required by court order are not subject to the minimum necessary rule. For example, the Trust may disclose PHI pursuant to an administrative subpoena, but the PHI must be limited to that which has been authorized to be disclosed for the limited purpose given in connection with the subpoena.

2. PUBLIC HEALTH REASONS

The Trust may disclose PHI to public health authorities authorized by law to collect or receive PHI for the purpose of disease control or prevention. This includes but is not limited to the following:

a. Reporting disease or injury

b. Reporting vital events such as birth or death

c. Conduct of public health surveillance

d. Conduct of public health investigations

e. Conduct of public health interventions

The Trust may disclose PHI at the direction of a public health authority to an officer of a foreign government agency that is acting in collaboration with a public health authority.

3. CHILD ABUSE OR NEGLECT

The Trust may disclose PHI to public health authorities or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

4. VICTIMS OF ABUSE, NEGLECT OR DOMESTIC VIOLENCE

The Trust will disclose PHI about an individual whom the Trust reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence.

The Trust must inform the individual of any disclosure under this Section 4 unless the insurer or the administrator believe informing the individual would place the individual at risk of serious harm, or if the insurer or the administrator would be informing a personal representative who they believe is responsible for the abuse or injury and informing the representative would not be in the best interests of the individual.

5. HEALTH OVERSIGHT ACTIVITIES

The Trust will disclose PHI to a health oversight agency for oversight activities authorized by law, such as audits; investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for oversight of:

a. the health care system;

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

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

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

The Trust will not disclose PHI for an investigation or other activity in which the individual is the subject of the investigation and the investigation is not related to the receipt of health care, a claim for public benefits related to health, qualification for or receipt of public benefits or services when a patient's health is integral to the public benefits or services.

Health oversight agencies include an agency or authority of the United States, including the Department of Labor, a State, a territory, a political subdivision of a state or territory, or an Indian tribe that is authorized by law to oversee the health care system (both public and private) or government programs described in this Section.

6. DISCLOSURE IN RESPONSE TO A COURT ORDER

The Trust will disclose PHI in the course of any judicial or administrative proceeding in response to an order of a court or administrative tribunal. The Trust will disclose only the PHI expressly authorized by such order.

7. DISCLOSURE IN THE COURSE OF JUDICIAL OR ADMINISTRATIVE PROCEEDING WITHOUT A COURT ORDER

The Trust will not disclose PHI in response to a subpoena, discovery request or other lawful process unless the insurer or the administrator verifies that the individual is aware of the request and has not made a valid objection to it, in accordance with the rules set forth in this Section.

Counsel will be consulted when a subpoena, discovery request, or other lawful process is received to determine whether the request for PHI is consistent with the underlying purpose for issuing the subpoena or other discovery request.

The Trust will disclose PHI in response to a subpoena, discovery request, or other lawful process, not accompanied by an order of a court or administrative tribunal, only if the Trust receives written documentation from the party seeking the PHI that reasonable efforts have been made to ensure that the individual who is the subject of the PHI has been given notice of the request and either did not object or a court overruled the objection.

Written documentation means a statement by the requestor that:

a. The party requesting disclosure has made a good faith attempt to provide written notice to the individual whose PHI is being sought, or if the individual's location is unknown, has mailed a notice to the individual's last known address;

b. The notice included sufficient information to allow the individual to go to court and object to the release; and

c. The time for objections has expired or the court has resolved the objections.

The Trust will also disclose PHI in response to a subpoena, discovery request, or other lawful process if the parties have agreed to a qualified protective order and have presented it to a court or administrative tribunal, or if the party seeking the PHI has requested a qualified protective order from such a court or administrative tribunal. A qualified protective order means an order of a court or administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested. It must also require the return or destruction of the PHI (including all copies made) at the end of the proceeding.

8. LAW ENFORCEMENT PURPOSES

The Trust will disclose PHI for a law enforcement purpose to a law enforcement officer. The Privacy Officer will be responsible for this disclosure and must take reasonable steps to verify that an individual is a member of a law enforcement entity.

The Trust will disclose PHI as required by and as relevant to the following legal process:

a. A court order, court-ordered warrant or subpoena, or summons issued by a judicial officer,

b. A grand jury subpoena, or

c. An administrative request, including an administrative subpoena or summons, or a civil or an authorized investigative demand, or similar process under law, if the PHI sought is relevant to a legitimate law enforcement inquiry, the request is specific and limited to the purpose for which the information is sought, and certification is made that de-identified information could not be used.

The Trust will disclose PHI about an individual in response to a law enforcement officer's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, but the Trust will supply only the following information:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and
h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

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

9. PHI OF VICTIMS

The Trust will disclose PHI in response to a law enforcement officer's request about an individual who is or is suspected to be a victim of a crime if:

a. The individual agrees to such disclosure, or
b. If the individual is unable to agree due to incapacity or other emergency circumstance, the law enforcement officer must represent that PHI is needed to determine whether a violation of law by someone other than the victim has occurred, and that such information is not intended to be used against the victim, that immediate law enforcement activity which depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and that disclosure is in the best, interests of the person.

The Trust will also disclose PHI about a deceased individual to law enforcement authorities if the insurer or the administrator suspects the individual's death resulted from a criminal act.

The Trust will disclose PHI if the insurer or the administrator has a good faith belief that it is evidence of a crime on their premises.

10. OTHER ENTITIES

The Trust will provide PHI to a coroner or medical examiner for the purpose of identification of a deceased person, determination of cause of death, or the coroner's other duties as authorized by law.

The Trust will also disclose PHI to funeral directors as necessary for fulfillment of their duties. If necessary, PHI may be disclosed prior to and in anticipation of the individual's death.

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

11. NATIONAL SECURITY

The Trust will disclose to the US Armed Forces PHI of individuals serving in the armed forces when deemed necessary by military authorities to assure execution of the military mission, if the military authority has published in the Federal Register the following information:

a. Appropriate military command authorities; and

b. The purposes for which the PHI may be used or disclosed.

The Trust will disclose PHI to authorized federal officers for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.)* and implementing authority. The Trust will also disclose PHI to officers for the protection of the

President or other persons or to foreign heads of state.

12. INMATES

The Trust will disclose PHI to correctional institutions and other law enforcement custodial situations if law enforcement represents that PHI is necessary for the provision of health care to the individual. The Trust will also disclose if necessary for the health and safety of the individual or others at the correctional institution or other persons responsible for the transportation of inmates and maintenance of safety, security, and order of the correctional institution. An individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

13. HEALTH PLANS

A health plan that is a state or local government program providing public benefits may disclose PHI relating to eligibility or enrollment in the health plan to another government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies is authorized by statute, is necessary to coordinate the covered functions of such programs, or is necessary to improve management of such programs.

14. WORKERS' COMPENSATION

The Trust may disclose PHI as authorized and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. Workers' compensation disclosures that are required by law are not subject to the minimum necessary rule.

15. COMPLIANCE WITH HIPAA

The Trust must permit HHS access during normal business hours to its facilities and information, including PHI that is pertinent to ascertaining compliance with the applicable requirements of HIPAA. If HHS determines that exigent circumstances exist, such as the destruction of documents, The Trust must permit access at any time without notice. Disclosures made to HHS in accordance with a HIPAA compliance investigation are not subject to the minimum necessary rule.

If any information required of the Trust under this Section is in the exclusive possession of any other agency or person and the other agency or person fails or refuses to furnish the information, the insurer or the administrator must set forth what efforts have been made to obtain the information.

3.2 PROCEDURES

1. Disclosures of Protected Health Information (PHI) without the authorization of the individual may be made according to the Trust's policies.

2. A request to inspect and/or copy PHI must be made on the form provided by the Trust. (See Request for Access to PHI Without Authorization From Individual Form.)

3. Requests from public officers shall be verified using the Trust's Verification Policy and Procedures for requests from public officers.

4. The form requesting the right to inspect and/or copy will be date-stamped by the Privacy Officer (or designee) and will be logged in.

5. The Trust may charge the following fees:

    a. Costs of copying PHI including labor and supplies,
    b. Postage for mailing the PHI, and
    c. The cost of preparing a summary of PHI.

6. The insurer or the administrator will record the following information in its files with a copy of the request form:

    a. The date the information was disclosed
    b. The information disclosed
    c. The requesting party's name and address
    d. The reason for the disclosure
    e. A copy of the subpoena, court order, etc. if applicable

REQUEST FOR ACCESS TO PHI WITHOUT AUTHORIZATION FROM INDIVIDUAL FORM

Name of Individual for whom PHI is requested: _____

Name of Party Requesting: _____

Address: _____

_____

I am requesting that I be allowed to inspect and copy the following PHI:

_____

_____

_____

_____

_____

Reason for Request of PHI:

_____

_____

Signature of Individual Requesting Access to PHI: _____

Attach copy of individual's identification to this form along with all other documentation of the reason for disclosure. (e.g. subpoena, court order, etc.)

4. CERTIFICATION & PLAN DOCUMENT AMENDMENT

4.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.504(f) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

CERTIFICATION POLICY

A plan sponsor, who is a participating employer in the Trust may certify to the Trust that it is in compliance with the Privacy Rules. The certification will allow the Trust to disclose individually identifiable health information to the plan sponsor for administration functions only. However, certification is not required if the Trust has entered into a Business Associate Agreement with the plan sponsor or if the plan sponsor is part of an organized health care arrangement with the Trust.

Organized health care arrangements include relationships between group health plans and their insurers and HMOs.

The Trust can disclose PHI to plan sponsors if plan sponsors voluntarily agree to use and disclose the information only as permitted or required by the regulation. The information may be used only for the Trust administration functions performed on behalf of the group health plan, which are specified in plan documents. Trust administration functions include quality assurance, claims processing, auditing, monitoring, and management of carve-out plans such as vision and dental. It does not include any employment-related functions or functions in connection with any other benefits or benefit plans, and group health plans may not disclose information for such purposes absent an authorization from the individual.

The Trust is not required to have a Business Associate Agreement in place with plan sponsors if the plan documents are amended to:

1. Describe the permitted uses and disclosures of PHI,

2. Specify that disclosure is permitted only upon receipt of a certification from the plan sponsor that the plan documents have been amended and the plan sponsor has agreed to certain conditions regarding the use and disclosure of PHI, and

3. Provide adequate firewalls to:

   (i) Identify the employees or classes of employees who will have access to PHI;

   (ii) Restrict access solely to the employees identified and only for the functions performed on behalf of the group health plan; and

   (iii) Provide a mechanism for resolving issues of noncompliance.

Additionally, a plan sponsor must certify to the Trust that the plan sponsor agrees to:

1. Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
2. Ensure that any subcontractors or agents to whom the plan sponsor provides PHI agree to the same restrictions;
3. Not use or disclose the PHI for employment-related actions or for use by other employee benefit plans;
4. Report to the Trust any use or disclosure that is inconsistent with the plan documents or the HIPAA privacy regulations;
5. Make the PHI accessible to individuals;
6. Allow individuals to amend their information;
7. Provide an accounting of its disclosures;
8. Make its practices available to the Secretary of HHS for determining compliance;

9. Return and destroy all PHI when no longer needed, if feasible; and
10. Ensure that the firewalls have been established.

SAMPLE CERTIFICATION TO GROUP HEALTH PLAN, HMO OR HEALTH INSURANCE ISSUER

This certification is intended to comply with the HIPAA Privacy Rules, 45 CFR 164.504(0 and 65 Fed. Reg. 82508 (December 28, 2000). This certification allows a participating employer ("Plan Sponsor") and The Tongass Timber Trust (the "Trust") to exchange protected health information for the Trust's administration functions without obtaining individual consent or authorization.

WHEREAS the _____is the sponsor of a group health plan under the Trust for its participants and their dependents; and

WHEREAS the Trust is a "health plan" within the meaning of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and

WHEREAS The Trust provides health insurance coverage to the participants and beneficiaries in the Plan Sponsor's group health plan; and

WHEREAS the Trust and Plan Sponsor desire to exchange health information protected under HIPAA ("protected health information or PHI") for purposes related to administration of the group health plan;

THEREFORE BE IT RESOLVED that Plan Sponsor hereby certifies to the Trust the following, as required by Section 45 CFR 164.504(f) of HIPAA:

The plan documents that govern Plan Sponsor's group health plan have been amended to incorporate the following provisions and Plan Sponsor agrees to:

- Not use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
- Ensure that any agents, including subcontractors, to whom it provides PHI received from Health Plan agree to the same restrictions and conditions that apply to Plan Sponsor with respect to such information;
- Not use or disclose PHI for employment-related actions and decisions;
- Not use or disclose PHI in connection with any other benefit or employee benefit plan of Plan Sponsor;
- Report to the Trust any PHI use or disclosure that it becomes aware of which is inconsistent with the uses or disclosures described in the plan documents as amended;
- Make PHI available to an individual based on HIPAA's access requirements;
- Make PHI available for amendment and incorporate any PHI amendments based on HIPAA's amendment requirements;
- Make available the information required to provide an accounting of disclosures;
- Make its internal practices, books and records relating to the use and disclosure of PHI received from the Trust available to the Secretary of the U.S. Department of Health and Human Services to determine the Trust's compliance with HIPAA;
- Ensure that adequate separation between the Trust and the Plan Sponsor and the Plan Sponsor's group health plan is established as required by HIPAA (45 CFR 164.504(f)(2)(iii)); and

- If feasible, return or destroy all PHI received from the Trust that Plan Sponsor still maintains in any form and retain no copies of such PHI when no longer needed for the specified disclosure purpose. If return or destruction is not feasible, Plan Sponsor will limit further uses and disclosures to those purposes that make the return or destruction infeasible.

Name of Employer: _____

By: _____

Title: _____

PLAN DOCUMENT AMENDMENT

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

A. The Plan will use protected health information to the extent and in accordance with the uses and disclosures permitted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Specifically, the Plan will use and disclose protected health information for purposes related to health care treatment, payment for health care, and health care operations.

1. Payment. "Payment" includes activities undertaken by the Plan to obtain premiums or determine or fulfill its responsibility for coverage and provision of Plan benefits that relate to an individual to whom health care is provided. These activities include, but are not limited to, the following:

   a. Determination of eligibility, coverage, and cost sharing amounts (e.g. cost of a benefit, Plan maximums, and co-payments as determined for an individual's claim),
   b. Coordination of benefits,
   c. Adjudication of health benefit claims (including appeals and other payment disputes),
   d. Subrogation of health benefit claims,
   e. Establishing employee contributions,
   f. Risk adjusting amounts due based on enrollee health status and demographic characteristics,
   g. Billing, collection activities and related health care data processing,
   h. Claims management and related health care data processing, including auditing payments, investigating and resolving payment disputes and responding to participant inquiries about payments,
   i. Obtaining payment under a contract for reinsurance (including stop-loss and excess of loss insurance).
   j. Medical necessity reviews, or reviews of appropriateness of care or justification of charges,
   k. Utilization review, including precertification, preauthorization, concurrent review and retrospective review,
   l. Disclosure to consumer reporting agencies related to collection of premiums or reimbursement (the following PHI may be disclosed for payment purposes: name and address, date of birth, SSN, payment history, account number, and name and address of the provider and/or health Plan), and
   m. Reimbursement to the Plan.

2. Health Care Operations. "Health Care Operations" include, but are not limited to, the following activities:

   a. Quality Assessment,
   b. Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, disease management, contacting of health care providers and patients with information about treatment alternatives and related functions,
   c. Rating provider and Plan performance, including accreditation, certification, licensing, or credentialing activities,
   d. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance),
   e. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs,
   f. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies,
   g. Business management and general administrative activities of the entity, including, but not limited to:
   h. Management activities relating to implementation of and compliance with the requirements of

HIPAA Administrative Simplification,

i. Customer service, including the provision of data analyses for policyholders, Plan sponsors, or other customers,
j. Resolution of internal grievances, and
k. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity.
l. Compliance with and preparation of all documents as required by the Employee Retirement Income Security Act of 1974 (ERISA), including Form 5500's, SAR's, and other documents.

B. The Plan will use and disclose PHI as required by law and as permitted by authorization of the participant or beneficiary. With an authorization, the Plan will disclose PHI to the pension plan and disability plan *[Note: list other plans to which information may be disclosed]* for purposes related to administration of those plans.

C. For purposes of this Amendment, the Employer is the "Plan Sponsor." The Plan will disclose PHI to the Plan Sponsor only upon receipt of a certification from the Plan Sponsor that the Plan documents have been amended to incorporate the following provisions.

D. With respect to PHI, the Plan Sponsor agrees to:

1. Not use or further disclose the information other than as permitted or required by the Plan Document or as required by law,
2. Ensure that any agents, including a subcontractor, to whom the Plan Sponsor provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Plan Sponsor with respect to such information,
3. Not use or disclose the information for employment-related actions and decisions unless authorized by the individual,
4. Not use or disclose the information in connection with any other benefit or employee benefit Plan of the Plan Sponsor unless authorized by the individual,
5. Report to the Plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware,
6. Make PHI available to the individual in accordance with the access requirements of HIPAA,
7. Make PHI available for amendment and incorporate any amendments to PHI in accordance with HIPAA,
8. Make available the information required to provide an accounting of disclosures,
9. Make internal practices, books, and records relating to the use and disclosure of PHI received from the group health Plan available to the Secretary of HHS for the purposes of determining compliance by the Plan with HIPAA, and
10. If feasible, return or destroy all PHI received from the Plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made. If return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction infeasible.

E. Adequate separation between the Plan and the Plan Sponsor must be maintained. Therefore, in accordance with HIPAA, only the following persons may be given access to PHI:

1. The administrator;
2. Claims staff at the insurer; and
3. Others:_____ *[NOTE. Please indicate which staff or persons should be included in this list by title or job function.]*

F. The persons described in section E may only have access to and use and disclose PHI for Plan administration functions that the Plan Sponsor performs for the Plan.

G. If the persons described in section E do not comply with this Plan Document, the Plan Sponsor shall provide a mechanism for resolving issues of noncompliance, including disciplinary sanctions.

H. For purposes of complying with the HIPAA privacy rules, if this Plan is a "hybrid entity" because it has both health plan and non-health plan functions, this Plan designates that its health care components that are covered by the privacy rules include only health benefits and not other plan functions or benefits.

5. DE-IDENTIFICATION

5.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

DE-IDENTIFICATION POLICY

The Trust may disclose health information that has been "de-identified" without observing other HIPAA-required policies and procedures, because de-identified information is not subject to the HIPAA privacy rules.

Health information that does not identify an individual, that complies with the de-identification policies and procedures, and which the Trust believes cannot be used to identify an individual is considered "de-identified."

If reasonable, to the extent possible, the Trust will use de-identified information for administration purposes.

5.2 PROCEDURES

DE-INDENTIFIED INFORMATION DESCRIBED:

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

a. Names;
b. All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip codes. The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. If the geographic units, which make up the initial three digits of a zip code contain 20,000 or fewer people, the first three digits must be changed to 000.
c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
d. Telephone numbers;
e. Fax numbers;
f. Electronic mail addresses;
g. Social security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;
m. Vehicle identifiers and serial numbers, including license plate numbers;
n. Device identifiers and serial numbers;
o. Web Universal Resource Locators (URLs);
p. Internet Protocol (IP) address numbers;
q. Biometric identifiers, including finger and voiceprints;
r. Full face photographic images and any comparable images; and
s. Any other unique identifying number, characteristic, or code, except as permitted for re-identification of the data as set forth below.

REIDENTIFITION: The Trust may assign a code or other means of record identification to allow de-

identified information to be re-identified by the insurer or administrator provided that:

a. Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
b. Security. The Trust does not use or disclose the code or other means of record identification for any other purpose, and do not disclose the mechanism for re-identification.

6. VERIFICATION

6.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.514(h) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

VERIFICATION POLICY

This policy is adopted pursuant to section 164.514(h) of the privacy regulations under the Health Insurance Portability and Accountability Act of 1996.

1. General Policy

It is the policy of the Trust to verify the identity of an individual or entity requesting Protected Health Information (PHI), and to verify the authority of such individual to have access to PHI, before the PHI is disclosed to the individual, if the identity or any such authority of the individual is not known to the insurer or the administrator.

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

2. Public Officers:

a. **Administrative Requests from Law Enforcement Officers:** If all of the conditions required before the Trust can disclose information to a law enforcement Officer pursuant to an administrative request are met, then the verification requirements are satisfied by the administrative subpoena or similar process, or by a separate written statement that, on its face demonstrates that the applicable requirements have been met. No additional verification is required. See Law Enforcement Policy and Privacy regulation section 164.512(f)(1)(ii)(C).
b. **Identity & Authority of Other Public Officers:** The identity and authority of all other public officers must be verified in the manner set out in the Trust's Verification Procedure for public officers.

3. Imminent Serious Threat of Health and Safety

A disclosure to an individual or entity pursuant to section 164.512(j)(1)(i) (other than to a public officer) to avert an imminent threat to health or safety is allowed without further verification if the insurer or the administrator has a good faith belief that the disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public, and the disclosure is to a person reasonably able to prevent or lessen the threat. If these conditions are met no further verification is needed. In such emergencies the insurer or the administrator are not required to demand written proof that the person requesting the PHI is legally authorized. the insurer or the administrator can reasonably rely on verbal representations.

4. Verification Procedures Under Section 510(b) of HIPAA

This policy does not apply to disclosures made under section 164.5i0(b) of HIPAA's privacy regulation regarding disclosures for facility directories, and disclosures for involvement in an individual's care or payment for care and for notification purposes. Verification procedures for persons requesting PHI under those circumstances are described in Section 8 of these Policies and Procedures.

6.2 PROCEDURES

When Required

Subject to any exceptions noted in the Trust's verification policy, unless an individual or entity is requesting PHI in person and the identity and authority of the individual or entity is personally known to the insurer or the administrator, the insurer or administrator must verify the identity and authority of the individual. Individuals are deemed to have the authority to obtain their own PHI, unless otherwise indicated.

General Policy

PHI will not be disclosed to an individual requesting this information on behalf of another, unless the individual is a personal representative of the individual (as set out in the Trust's Personal Representative Policy and Procedure) or an authorization is on file. The administrator and the insurer will confirm the authority of a person to act on behalf of the individual by making sure that a personal representative form or other legal document or an authorization has been properly filed with the Privacy Officer indicating the authority of the individual to act on behalf of another. Parents/guardians of minor children are deemed to be the personal representative of their minor children.

Request by Mail or Fax for Individual's Own PHI:

Any request for disclosure of PHI by mail or fax must be made in writing on the Trust's Request for Access to PHI form. The information will be sent to the participant's last known address, unless a written change of address form has been received or a request that PHI be transmitted by alternative means is on file.

1. VERIFICATION PROCEDURES FOR THE INSURER

The insurer will refer all inquiries regarding eligibility to the administrator.

- **MANNER OF VERIFYING IDENTITY WHEN REQUESTING OWN PHI**

  - **Request in Person for Individual's Own PHI:**

    If an individual makes a request for their own PHI in person, they must show the insurer at least one piece of photo identification such as: driver's license or passport to verify their identity.

  - **Request by Telephone for Individual's Own PHI**

    The insurer responding to a request by telephone for an individual's own PHI where the request involves status of a specific claim as paid or not paid must verify the individual's identity by asking them to verify the following information in their file:

    - Social Security number of participant, or
    - Name and date of birth of participant, and
    - One additional piece of information such as:
      - Address
      - Home phone number

    If caller is a dependent they must also provide:
    - Name of dependent
    - Date of birth of dependent

- **MANNER OF VERIFYING IDENTITY WHEN REQUESTING PHI ON BEHALF OF ANOTHER**

  - **Requests in Person on Behalf of Another - Parent/guardian of Minor Child:**

    Parents/guardians of minor children must show at least one piece of photo identification, such

as a driver's license or passport, and verify their relationship to the individual by providing:

- Social Security number of participant, or
- Name and date of birth of participant, and
- Name of minor child
- Date of birth of minor child

- **Requests in Person on Behalf of Another - Personal Representatives or Authorization:**

  Personal representatives must show at least one piece of photo identification, such as a driver's license or passport and verify their relationship to the individual by providing:

  - Social Security number of participant, or
  - Name and date of birth of participant, and
  - Name of individual
  - Date of birth of individual

  The insurer will then refer to the notes placed on the system at the time the personal representative document or authorization was received and ask the person requesting PHI to verify two other pieces of information which the Privacy Officer or designee determined from the personal representative document or authorization to be satisfactory identifying information; for example, the date of the claim which is the subject of the authorization or relationship of personal representative to the individual.

- **Requests by Telephone on Behalf of Another - Parent/guardian of Minor Child:**

  Parents/guardians requesting PHI of minor children by telephone must verify their identity by providing the following information:

  - Social Security Number of participant
  - Name of participant
  - Name of minor child
  - Date of birth of minor child

- **Requests by Telephone on Behalf of Another - Personal Representative or Authorization:**

  Personal representatives, or authorized individuals requesting PHI by telephone must verify their identity and their relationship to the individual by providing the following pieces of information:

  - Social Security Number of participant
  - Name of participant
  - Name of individual
  - Date of birth of individual

  The insurer will then refer to the notes placed on the system at the time the personal representative document or authorization was received and ask the person requesting PHI to verify two other pieces of information which the Privacy Officer or designee determined from the personal representative document or authorization to be satisfactory identifying information, such as date of claim that is the subject of the authorization.

2. VERIFICATION PROCEDURES FOR THE ADMINISTRATOR

Except when participants have requested assistance from the administrator on a specific claim, the administrator will refer inquiries regarding claims to the insurer.

- **MANNER OF VERIFYING IDENTITY WHEN REQUESTING OWN PHI**

  - **Request in Person for Individual's Own PHI:**

    If an individual makes a request for their own PHI in person, they must show the administrator at least one piece of photo identification such as: driver's license or passport to verify their identity. They must also provide the name and social security number of the participant.

  - **Request by Telephone for Individual's Own PHI**

    The administrator responding to a request by telephone for an individual's own PHI must verify the individual's identity by asking them to verify the following information in their file:

    - Social Security number of participant, or
    - Name and date of birth of participant, and
    - One additional piece of information, such as:
      - Address
      - Home phone number

    If caller is a dependent they must also provide:

    - Name of dependent
    - Date of birth of dependent

- **MANNER OF VERIFYING IDENTITY WHEN REQUESTING PHI ON BEHALF OF ANOTHER**

  - **Requests in Person on Behalf of Another - Parent/guardian of Minor Child:**

    Parents/guardians of minor children must show at least one piece of photo identification, such as a driver's license or passport, and verify their relationship to the individual by providing:

    - Social Security Number of participant, or
    - Name and date of birth of participant, and
    - Name of minor child
    - Date of birth of minor child

  - **Requests in Person on Behalf of Another - Personal Representatives or Authorization:**

    Personal representatives must show at least one piece of photo identification, such as a driver's license or passport and verify their relationship to the individual by providing:

    - Social Security Number of participant, or
    - Name and date of birth of participant, and
    - Name of individual
    - Date of birth of individual

The administrator will then refer to the notes placed on the system at the time the personal representative document or authorization was received and ask the person requesting PHI to verify two other pieces of information which the Privacy Officer or designee determined from the personal representative document or authorization to be satisfactory identifying information; for example, the date of the claim which is the subject of the authorization or relationship of personal representative to the individual.

  - **Requests by Telephone on Behalf of Another - Parent/guardian of Minor Child:**

    Parents/guardians requesting PHI of minor children by telephone must verify their identity by providing the following information:

    - Social Security Number of participant

- Name of participant
- Name of minor child
- Date of birth of minor child

o **Requests by Telephone on Behalf of Another -Personal Representative or Authorization:**

Personal representatives or authorized individuals requesting PHI by telephone must verify their identity and their relationship to the individual by providing the following pieces of information:

- Social Security Number of participant
- Name of participant
- Name of individual
- Date of birth of individual

The administrator will then refer to the notes placed on the system at the time the personal representative document or authorization was received and ask the person requesting PHI to verify two other pieces of information which the Privacy Officer or designee determined from the personal representative document or authorization to be satisfactory identifying information, such as date of claim that is the subject of the authorization.

3. REQUESTS INVOLVING A TRANSLATOR:

If an individual requests that a translator assist them in discussing PHI with the insurer or the administrator, the Trust shall either obtain an authorization (and verify identity of the translator) or follow the procedure set forth in the Trust's Policy for Involvement in an Individual's Care or Payment for Care (see Section 8 of these Policies and Procedures).

4. REQUESTS BY HEALTH CARE PROVIDERS:

PHI will be disclosed to a health care provider for purposes related to the payment or health care operations of the Trust. If the health care provider calls via telephone, the insurer and the administrator will disclose PHI after the following steps:

- The health care provider must state his or her name and provider tax identification number.
- If the inquiry involves a claim, the administrator will refer it to the insurer.
- The health care provider must identify four of the following five pieces of information:
  - Name of participant
  - Social Security Number of participant
  - Name of patient
  - Date of birth of patient
  - Date of service

5. REQUESTS BY PUBLIC OFFICERS:

a. Identifying Public Officer

The insurer or the administrator will rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity of a public officer or a person acting on behalf of a public officer:

- If the request is made in person, presentation of an agency identification badge, other officer credential, or other proof of government status;
- If the request is in writing, the request is on appropriate letterhead; or
- If the disclosure is to a person acting on behalf of a public officer, a written statement on

appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract or memorandum of understanding, that establishes that the person is acting on behalf of the public officer.

b. Confirming Authority of Public Officer

The insurer or the administrator may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public officer or a person acting on behalf of the public officer (this confirmation cannot be completed via telephone):

- A written statement of the legal authority under which the PHI is requested, or if a written statement is impractical, an oral statement of such legal authority;
- A request made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal is presumed to constitute legal authority.

6. REQUESTS BY OTHER PARTIES:

When an entity other than the individual themselves, a personal representative, or public officer requests disclosure of PHI that is otherwise allowed under HIPAA and the Trust's Policies and Procedures, their identity and authority must also be confirmed. An entity will have the authority to receive the information if a valid authorization is completed pursuant to the Trust's authorization policy. For any other entity described in the Trust's policy for disclosure of PHI for public health, law enforcement, or legal process, the authority and identity of the entity must be confirmed in writing on letterhead to the insurer or the administrator that the entity is who they claim to be. The entity must also provide a written statement describing the authority under which the PHI is requested.

7. RECOGNITION OF PERSONAL REPRESENTATIVE

7.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and pursuant to section 2560.503-1 of the claims and appeals regulation under the Employment Retirement Income Security Act ("ERISA").

RECOGNITION OF PERSONAL REPRESENTATIVE

1. The Trust will treat a personal representative as the individual for purposes of implementing the HIPAA privacy rules and ERISA's claims and appeals procedure rules.

    a. The personal representative may only have access to PHI that is consistent with and relevant to the scope of authority set out in the personal representative form.

    b. The Trust may elect not to treat a person as the personal representative of an individual if:

        (1) The insurer or the administrator has a reasonable belief that:

            - The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
            - Treating such person as the personal representative could endanger the individual; and

        (2) The insurer or the administrator, in the exercise of professional judgment, decide that it is not in the best interest of the individual to treat the person as the individual's personal representative.

2. The following individuals will be deemed to be a personal representative of an individual without having to complete a personal representative form, unless the Trust agrees to a request by an individual to restrict disclosure of PHI to the deemed personal representative under section 164.522 of the privacy regulation:

    a. **PARENTS/GUARDIANS OF UNEMANCIPATED MINORS:** The Trust will consider a parent or guardian as the personal representative of an unemancipated minor unless applicable law requires otherwise, or the Trust agrees to abide by a participant or beneficiary request that the Trust restrict disclosure of PHI to a parent or guardian.

    b. **DECEASED INDIVIDUALS:** The Trust will automatically recognize the following persons as personal representatives of deceased individuals or their estates:

        - Executors
        - Administrators
        - Other persons with authority to act on behalf of the deceased individual or their estate.

    c. **TREATING PHYSICIAN REGARDING AN URGENT CLAIM: In** the case of an "urgent claim," a "health care professional" (as these terms are defined in ERISA's claims regulation) with knowledge Of a participant or beneficiaries medical condition will be automatically recognized by the Trust as a personal representative. The health care professional is deemed to be a personal representative only with respect to the disclosure of PHI directly relating to the urgent claim.

    d. **POWER OF ATTORNEY:** The Trust will automatically recognize any person who holds a legal power of attorney for an individual as that individual's personal representative.

    e. **OTHER APPLICABLE LAW:** The Trust will recognize any person who is authorized under State or other applicable law (e.g. court-appointed legal guardian) to act on behalf of the individual in making health care related decisions as that individual's personal representative.

3. The Trust may disclose PHI to an individual who is not a personal representative (or deemed to be a personal representative) if they are a family member, other relative or close personal friend of the individual, or any other person identified by the individual, and the disclosure is directly relevant to such person's involvement with the individual's care or payment for the individual's care pursuant to sections 164.510(b) of HIPAA's privacy regulation. See The Trust's Policy and Procedure for Uses and Disclosures for Involvement in an Individual's Care or Payment for Care and for Notification Purposes.

4. The Trust will make available a form which can be used to designate a personal representative for purposes of receiving protected health information related to claims for coverage or benefits under the Plan and exercising any individual rights regarding protected health information under HIPAA. Where a personal representative form has been completed and approved by the Privacy Officer, it will be recognized by the Trust as long as the individual making the designation is covered by the Trust. The individual has a right to revoke the designation at any time by submitting a signed statement to the administrator revoking the designation. To designate another individual as personal representative, a new personal representative form must be completed and approved by the Privacy Officer.

7.2 PROCEDURES

Other than those individuals deemed to be personal representatives in paragraph 2 of the Policies related hereto, The Trust will only treat an individual as a personal representative where a personal representative document has been filed with the Privacy Officer and been approved. The Privacy Officer may request the assistance of the Trust counsel in making this determination.

Individuals may request a copy of the personal representative form by calling the administrator at (907) 225-6114. All personal representatives will be subject to the Trust's verification procedure.

APPOINTMENT OF PERSONAL REPRESENTATIVE FORM
(Sample Form)

(Please Print)

I. Information Regarding Participant or Beneficiary

I, _____
(Name of Participant or Beneficiary)

Mailing Address: _____

Social Security Number: _____

Date of Birth: _____ Phone:_____

II. Designation Of Personal Representative

❒ Hereby designate: _____
(Name of Personal Representative)
to act on my behalf.

I authorize my Personal Representative to receive any information that is (or would be) provided to me as a Participant/Beneficiary of the Plan, including but not limited to, any information that relates to my claim for coverage or benefits under the Plan and any individual rights that I have regarding my protected health information under HIPAA (Health Insurance Portability and Accountability Act of 1996).

Personal Representative's
Relationship to participant/Beneficiary: _____

III. Designation of Personal Representative for Dependent

❒ Hereby designate: _____
(Name of Personal Representative)

to act on behalf of: _____
(Name of Dependent)

(This designation may be made by a parent or guardian of a minor, or by the guardian or conservator of an adult individual)

I authorize my Dependent's Personal Representative to receive any information that is (or would be) provided to me as a Participant/Beneficiary of the Plan regarding my Dependent, including but not limited to, any information that relates to a claim for coverage or benefits under the Plan and any individual rights that I have regarding my Dependent's protected health information under HIPAA. I understand that under state law, there are circumstances in which a minor child's protected health information cannot be released to a parent, or to a Personal Representative acting on a parent's behalf.

Dependents
Relationship to
Participant/Beneficiary: _____

Personal Representative's
Relationship to Participant/Beneficiary: _____

Dependent's Mailing address: _____

Dependent's Social Security Number: _____

Dependent's Date of Birth: _____

Dependent's Phone: (__) _____

IV. Information Regarding the Personal Representative

Mailing Address: _____

Social Security Number: _____

Date of Birth: _____

Phone: (___) _____

V. Statement of Individual Rights

I understand that this designation is subject to approval by the Plan. I also understand that, once approved, this designation will remain in effect unless I revoke it. I understand that I have the right to revoke this designation at any time by submitting a signed statement to that effect to the administrator, attention Privacy Officer.

I also understand that Dependents may have their own rights by law and that one member of a family may not always have the authority to authorize the uses or disclosures of the protected health information of other family members

VI. Signatures:

_____ _____
Participant or Beneficiary's Signature Date

_____ _____
Personal Representative's Signature Date

8. USE & DISCLOSURE FOR INVOLVEMENT IN AN INDIVIDUAL'S CARE OR PAYMENT FOR CARE AND FOR NOTIFICATION PURPOSES

8.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.51(b) of the privacy rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

USE & DISCLOSURE FOR INVOLVEMENT IN AN INDIVIDUAL'S CARE AND FOR NOTIFICATION PURPOSES POLICY

The Trust may disclose to a family member, other relative, or a close personal friend of an individual, or to any other person identified by the individual, protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. This disclosure can only be made where the individual that is the subject of the PHI is given the opportunity to agree or object according to The Trust's Procedure for Use & Disclosure for Involvement in an Individual's Care or Payment for Care and for Notification Purposes.

The Trust may also use and disclose protected health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual, or another person responsible for the care of the individual, of the individual's location, general condition, or death. The general purpose of this rule is to allow disclosure in those limited instances where disclosure of protected information to next-of-kin (or to those with a close relationship to an individual) is necessary, or where it is needed in order to locate next-of-kin or other individuals involved in their care. This policy will also allow disclosure of protected health information to disaster relief organizations under certain circumstances.

Any such use or disclosure must be made according to The Trust's Procedure for Use & Disclosure for Involvement in an Individual's Care or Payment for Care and for Notification Purposes.

Disclosures made under this policy and procedure is not subject to The Trust's verification policy.

Exceptions

- This policy and procedure will not apply to disclosures to individuals who are personal representatives in accordance with the Trust's Recognition of Personal Representative Policy & Procedure.

- This policy and procedure does not apply to disclosures made to avert an imminent threat to health or safety, as described in section 8 of the Trust's Policy Regarding the Disclosure for Public Health, Law Enforcement, or Legal Process.

8.2 PROCEDURES

The following procedures must be followed before PHI is disclosed to a person involved in an individual's care or payment for care or for notification purposes:

1. Use or Disclosure with the Individual Present

If an individual is present, or otherwise available, prior to a use or disclosure to those involved in an individual's care or payment for care or for notification purposes, and the individual has the capacity to make health care decisions, the Trust may use or disclose protected health information if the Trust:

a. Obtains the individual's agreement (either orally or in writing)
b. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
c. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

This procedure may be followed when a translator accompanies an individual.

2. Limited Uses and Disclosures When the Individual is not Present

If an individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the insurer or the administrator may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care. The insurer or administrator may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interests in allowing a person to act on behalf of the individual in obtaining protected health information on their behalf to assist an individual in their care or payment for their care.

3. Use and Disclosure for Disaster Relief Purposes

The Trust may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted to notify or assist in notifying persons involved in an individual's care. Disclosures to these entities must be made according to Sections 1 and 2 above where the insurer or the administrator determines, in the exercise of their professional judgment that the requirements in Sections 1 and 2 do not interfere with the ability to respond to an emergency situation.

4. Documentation

All written agreements to allow disclosure or written objections to the disclosure must be kept according to the Trust's Record Retention Policy.

9. CLAIMS AND APPEALS

9.1 PRIVACY POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.502(g) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and pursuant to Section 2560.503-1 of the claims and appeals regulation under the Employee Retirement Income Security Act ("ERISA").

CLAIMS AND APPEALS POLICY

The Trust will safeguard the privacy of protected health information used and disclosed during the claims and appeal process by using and disclosing only the information that is minimally necessary to make claims determinations and appeals, and by limiting access to protected health information to only those appropriate individuals at the insurer, the administrator, and other service providers and business associates that need to review this information. See the Trust's Minimum Necessary Policy. In addition, in dealing with PHI involving health claims, the Trust will recognize all individuals' rights required by HIPAA and set forth in the Trust's Individual Rights Policies and Procedures.

9.2 PRIVACY PROCEDURES

The Trust, at a minimum; will incorporate the following procedures within the claims process:

1. Initial Claim Review: To be handled by the insurer.

2. Appeals: To be handled by the insurer.

3. Individual Inquiries on Claims: All inquiries concerning claims that involve the disclosure of PHI are subject to the Trust's Policy and Procedure to verify the identity and authority of the individual making the request. In addition, any Trust disclosure of PHI in response to inquiries made on behalf of another will only be made with an individual authorization, unless the individual requesting the PHI is a personal representative, or other individual where authorization is not required under the privacy regulation. All PHI concerning claims obtained in responding to individual inquiries will be safeguarded pursuant to the Trust's Security and Record Retention Policy and Procedure.

10. RIGHT TO REQUEST RESTRICTIONS ON USE & DISCLOSURE

10.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.522 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RIGHT TO REQUEST RESTRICTION OF USE & DISCLOSURE POLICY

A covered individual may request that the Trust restrict the use and disclosure of PHI for treatment, payment and heath care operations and to persons involved in an individual's care and for notification purposes.

The Trust, however, is not required to agree to the request if the Privacy Officer determines it to be unreasonable.

If the Trust agrees to the requested restriction, it will abide by the restriction except:

1. If the individual is in need of emergency treatment, and
2. The disclosure is necessary to provide that treatment,
3. The Trust may then use the restricted PHI, and may disclose this information to a health care provider in order to provide the needed treatment:

If restricted PHI is disclosed to a health care Provider because it is necessary for emergency treatment, the Trust will request that the health care provider not further use or disclose the information.

The Trust's agreement to a restriction on the use or disclosure is not effective to prevent uses or disclosures:

1. When required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with HIPAA,
2. For Facilities directories, or
3. For instances where an authorization is not required under the Trust's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.

The Trust's agreement to a restriction is binding only on the Trust and its Business Associates, not on other entities such as insurers or health care providers.

10.2 PROCEDURES

1. An individual covered by the Trust may request that the Trust restrict any use or disclosure of his/her PHI for treatment, payment and health care operations, and to persons involved in an individual’s care and for notification purposes. (See Request for Restriction Form.)

2. An individual must make a request to restrict the use or disclosure of PHI in writing to the following Privacy Officer:

   Privacy Officer
   (Address)
   (Telephone number)

3. The Privacy Officer will review the request and notify the covered individual in writing of the decision.

4. The Trust's agreement to a restriction on the use or disclosure is not effective to prevent uses or disclosures:

   a. When required by the Secretary of the U.S. Department of Health and Human Services to

investigate or determine compliance with HIPAA,

b. For Facilities directories, or
c. For instances where an authorization is not required under the Trust's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process.

5. The covered individual may revoke the Trust's agreement to restrict the use and disclosure of his/her PHI by submitting a signed written request to terminate the agreement.

6. The Trust may terminate an agreement to restrict the use and disclosure of PHI by notifying the covered individual in writing. The termination will only be effective for PHI created or received after the date the administrator sends the notice.

7. The Privacy Officer will retain documentation of the restrictions that are approved for six years.

PRIVACY PROTECTION REQUEST FORMS

REQUEST FOR RESTRICTIONS ON USE & DISCLOSURE FORM

Individuals should use this form to request a restriction on the use or disclosure of individual PHI.

DENIAL OF REQUEST FOR RESTRICTIONS ON USE & DISCLOSURE FORM

The Privacy Officer should use this form to:

- Notify the individual of the denial of the request for restriction, and
- Provide a statement of the individual's right to have the denial reviewed.

REQUEST FOR RESTRICTIONS ON USE & DISCLOSURE FORM
(Sample Form)

Date: _____

Name of Individual: _____

Address: _____

_____

Social Security Number: _____

I am requesting that use and access to my PHI be restricted in the following manner:

_____

_____

_____

_____

_____

_____

I understand that if agreed to, the Trust may not be able to honor this request if I require emergency medical treatment. I also understand that that the Trust may remove this restriction in the future, if I am notified in advance.

Signature of Individual Requesting Restriction: _____

Signature of Personal Representative
acting on behalf of the Individual,
if the Individual is not making the Request for Restriction _____

DENIAL OF REQUEST FOR RESTRICTION ON USE & DISCLOSURE FORM
(Sample Form)

Date: _____

Date of Request for Restriction on Protected Heath Information: _____

Name of Individual Requesting Restriction: _____

Your Request for Restriction on the use of disclosure of your Protected Health Information has been denied for the following reasons:

_____

_____

_____

_____

_____

_____

Signature of Privacy Officer: _____

11. RIGHT TO REQUEST INFORMATION BE TRANSMITTED BY ALTERNATIVE MEANS

11.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.522(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RIGHT TO REQUEST INFORMATION BE TRANSMITTED BY ALTERNATIVE MEANS POLICY

The Trust will permit and accommodate a covered individual's reasonable request to have PHI sent by alternative means or to an alternative location.

11.2 PROCEDURES

A covered individual may request the Trust to transmit PHI by an alternative means or to an alternative location.

The request must be in writing and mailed or faxed to the following address:

Privacy Officer
(Address)
(Telephone number)

Each request must be dated-stamped and logged in by the Privacy officer.

The Privacy Officer will review and notify the covered individual of whether the request will be honored.

The Trust will only accommodate a reasonable request. A request will be considered reasonable if the request is for mailing to a different address than the one to which it would otherwise be mailed. The alternative address must be specified in the request.

REQUEST FOR INFORMATION BE TRANSMITTED BY ALTERNATIVE MEANS FORMS

REQUEST THAT PHI BE TRANSMITTED BY ALTERNATIVE MEANS FORM

Individuals should use this form to request that PHI be transmitted by alternative means.

DENIAL OF REQUEST THAT PHI BE TRANSMITTED BY ALTERNATIVE MEANS FORM

The Privacy Officer should use this form to:

- Notify the individual of the denial of the request that PHI be transmitted by alternative means,
- Provide a statement of the individual's right to have the denial reviewed.

REQUEST THAT PHI BE TRANSMITTED BY ALTERNATIVE MEANS FORM
(Sample Form)

Date: _____

Name of Individual: _____

Address: _____

_____

Social Security Number: _____

I am requesting that my protected health information be transmitted to me by the following means:

A. Specify the information that you wish to be sent by alternative means:

_____

_____

B. Please provide the different address to which you would like the information to be sent

_____

_____

_____

_____

Signature of Individual requesting alternate transmission of PHI: _____

Signature of Personal Representative
acting on behalf of the Individual, if the Individual is
not making the Request for alternative transmission: _____

DENIAL OF REQUEST FORM THAT PHI BE TRANSMITTED BY ALTERNATIVE MEANS FORM
(Sample Form)

Date: _____

Date of Request that PHI be transmitted by alternate means: _____

Name of Individual Requesting alternate transmission of PHI:_____

Your request that PHI be transmitted by alternate means has been denied for the following reasons:

_____

_____

_____

_____

Signature of Privacy Officer: _____

12. RIGHT OF ACCESS TO PHI

12.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.524 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RIGHT OF ACCESS TO PHI POLICY

A covered individual has the right to inspect and obtain a copy of Protected Health Information (PHI) pertaining to the individual in a designated record set, except as otherwise provided in the law or provided in the Trust's Procedures for the Right of Access to PHI. The Trust may impose a reasonable cost-based fee for copying PHI or for preparing a summary of PHI.

The Trust will provide access to PHI only for as long as the PHI is maintained in a designated record set.

12.2 PROCEDURES

1. A covered individual under the Trust or a personal representative of such individual may make a written request to inspect and/or copy PHI pertaining to the covered individual in a designated record set.

2. "Designated record set" means a group of records maintained by or for the Trust that is: (a) the medical claims records and billing records about individuals received from health care providers; (b). the enrollment form, printout of eligibility screen, payment records, claim forms, claims adjudication printout screens, EOBs, and case or medical management records maintained by or for the Trust, including correspondence from members providers and collection notices; or (c) used, in whole or in part, by or for the Trust to make decisions about individuals.

   The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for the Trust. It does not include access to the databases of the Trust's Business Associates but only printout copies of screens related to the individual.

   In general, all records maintained by the insurer or the administrator relating to the individual covered under the Trust's enrollment, eligibility, claims, appeals, and related information are considered to be part of the designated record set for an individual. It shall not include records related to claims audits. The Privacy Officer or designee shall have ultimate responsibility for determining what constitutes the designated record set.

3. The following information will not be considered part of the designated record set made available for inspection or copying. Requests for access to this information will be denied:

   a. Psychotherapy notes,
   b. Copies of health information kept in multiple locations - only the original should be included in the designated record set.
   c. Information compiled in anticipation of, or for use in, a civil, criminal or administrative action or proceeding.
   d. PHI that was obtained under a promise of confidentiality (other than from a health care provider), where the access requested would be reasonably likely to reveal the source of the information.
   e. Quality improvement or risk management records.
   f. Research documentation while a clinical trial is taking place, if the individual who is part of the clinical trial agreed to denial of access upon participation.
   g. Appointment schedules.
   h. Information compiled in anticipation of a government or administrative proceeding.
   i. Cancer registry information.

4. The Trust will also deny the right to inspect and copy the PHI, if in the opinion of a licensed health

care professional, the access requested by the individual or their personal representative, is reasonably likely to cause substantial harm to the individual or another person. the Trust will also deny the right to inspect and copy protected health information that makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to such other person.

5. If access is denied for the reasons stated in paragraph 4, the individual has the right to have the denial promptly reviewed by a licensed health care professional designated as a reviewing official who did not participate in the original decision. the Trust will designate an unrelated and different licensed health care professional to act as the reviewing official in such cases. Denials for access for the reasons set out in paragraph 3 are not subject to review. the Trust will provide a written notice to the individual of a determination on review.

6. A request to inspect and/or copy PHI must be made on a form provided by the Trust and mailed to the following address. (See Request for Access to PHI Form.) All requests are subject to the Trust's Verification Policy.

   Privacy Officer
   (Address)
   (Telephone number)

7. The form requesting the right to inspect and/or copy will be date-stamped by the Privacy Officer and will be logged in.

8. If a personal representative makes the request, there must be a proper authorization on file pursuant to the Trust's Personal Authorization Policy.

9. The Privacy Officer will act on a properly filed request within 30 days of receipt of the request (60 days if the PHI is not maintained on-site).

   a. If the request is approved, the individual will be notified of the approval and access will be provided.
   b. If the request is denied, a written denial notice will be provided stating the basis for denial. For a denial notice concerning a denial for the reasons stated in paragraph 4, The Trust will also provide a statement of the right of the individual to have the denial reviewed and a description of how the individual may file a complaint with the Trust and the U.S. Department of Health and Human Services.
   c. The time for responding may be extended by 30 days if the Privacy Officer is unable to act upon the request and the individual is notified in writing of the need for extension within 30 days of receipt of the request.
   d. If the Trust does not maintain the protected health information that is the subject of the request, and the Trust knows where the requested information is maintained, it will inform the individual where to direct the request for access in the response to the request.

10. The Trust will provide the individual with access to the protected health information in a timely manner in the form or format requested by the individual, if it is readily producible in such form or format; or if not, in a readable hard copy form or such other form or format as agreed to by The Trust and the individual. In lieu of providing PHI, The Trust may provide a summary of the PHI requested if the individual agrees in advance to the summary and to any fees charged for the summary. the Trust may arrange with the individual for a convenient time or place to inspect or obtain a copy of the information, or mail a copy of the information at the individual's request.

11. The Trust will charge the following fees:

    a. Costs of copying PHI including labor and supplies,
    b. Postage for mailing the PHI, and
    c. The cost of preparing a summary of PHI.

12. The Trust will document the designated record set that is subject to access by individuals. It will also document the title of the individual responsible for receiving and processing requests for access by individuals. The Trust will also maintain any communication required by this procedure to be in writing (e.g. notice of denial).

RIGHT OF ACCESS TO PHI FORMS

REQUEST FOR ACCESS TO PHI FORM

Individuals should use this form to request access to individual PHI.

NOTICE OF EXTENSION OF TIME TO DETERMINE RIGHT TO ACCESS

The Privacy Officer should use this form to notify the individual requesting access that the deadline to act on the request for PHI is being extended by 30 days.

DENIAL OF REQUEST FOR ACCESS TO PHI FORM

The Privacy Officer should use this form to:

- Notify the individual of the denial of the request for access to PHI,
- Provide a statement of the individual's right to have the denial reviewed.

REQUEST FOR ACCESS TO PHI FORM
(Sample Form)

Date: _____

Name of Individual: _____

Address: _____

_____

Social Security Number:_____

I am requesting that I be allowed to inspect and copy the following PHI:

_____

_____

_____

_____

- ❑ I prefer to inspect, and/or copy, this information in person and will contact the administrator (phone 907-225-6114) to arrange a time.

- ❑ Please mail this information to me at the address above. (Note that if this is not the current address on file for you with the administrator you will be required to provide verification of the address.)

I understand that I may be charged a fee for the costs of copying, including labor and supplies, and postage. I also may be charged the cost of preparing a summary of protected health information, if such a summary is requested. I have reviewed the Trust's rules for access to information contained in the Trust's Notice of Privacy Practices.

Signature of Individual Requesting Access to PHI: _____

Signature of Personal Representative
acting on behalf of the Individual, if the Individual is not PHI: _____

NOTICE OF EXTENSION OF TIME TO DECIDE REQUEST FOR ACCESS TO PHI
(Sample Form)

Date: _____

Date of Request for Access to PHI: _____

Name of Individual Requesting Access: _____

A decision on your Request for Access to PHI that was received by the Trust on _____ will be delayed for _____ days [30 days or actual number, if less].

You will be notified of the decision on your Request at or before that time.

The decision is being delayed for the following reasons:

_____

_____

_____

_____

_____

_____

Signature of Privacy Officer: _____

DENIAL OF REQUEST FOR ACCESS TO PHI FORM
(Sample Form)

Date: _____

Date of Request for Access to PHI: _____

Name of Individual Requesting Access: _____

Your Request for Access to PHI has been denied for the following reasons:

_____

_____

_____

_____

In certain circumstances you have the right to have this denial reviewed. If the following paragraph applies to your request, the "Yes" box will be checked.

This denial is subject to appeal as described below: ❒ No ❒ Yes

You have the right to have this denial reviewed by a licensed health care professional designated by the Trust to act as a reviewing official and who did not participate in the original decision to deny. You can request a review by contacting the administrator in writing. If you request a review, the Trust will notify you within a reasonable time of the determination of the designated reviewing official and take action to carry-out the official's determination. You also have the right to file a complaint with the Trust or the Secretary of the U.S. Department of Health and Human Services, as outlined in the attached copy of the Trust's Privacy Notice.'

Privacy Officer Phone: _____

Signature of Privacy Officer: _____

13. RIGHT TO AMEND PHI

13.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.526 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RIGHT TO AMEND PHI POLICY

A covered individual has the right to have the Trust amend PHI or other information maintained in its designated record set subject to the exceptions set out in the Trust's Right to Amend PHI Procedures. If the Trust does not agree to amend the PHI, the individual has the right to submit a written statement disagreeing with the denial and explaining the basis for the disagreement. The Privacy Officer may then issue a rebuttal statement.

The right to amend PHI applies only for as tong as the PHI is maintained in a designated record set.

The Trust is not required to delete or expunge any PHI from their records under the privacy rules. Also The Right to Amend does not include the right for a covered individual to make the actual changes to PHI. Where a request to amend is accepted by the Trust, the Trust will determine the appropriate amendment (taking into account any suggested amendment from the individual).

13.2 PROCEDURES

A covered individual may request in writing that the Trust amend PHI pertaining to that individual. The PHI must be in a designated record set maintained by the Trust.

"Designated record set" means a group of records maintained by or for the Trust that is: (a) the medical claims records and billing records about individuals received from health care providers; (b) the enrollment form, printout of eligibility screen, payment records, claim forms, claims adjudication printout screens, EOBs, and case or medical management records maintained by or for the Trust, including correspondence from members providers and collection notices; or (c) used, in whole or in part, by or for the Trust to make decisions about individuals.

The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for the Trust. It does not include access to the databases of the Trust's Business Associates but only printout copies of screens related to the individual.

In general, all records maintained by the insurer or the administrator relating to the individual covered under the Trust's enrollment, eligibility, claims, appeals, and related information are considered to be part of the designated record set for an individual. It shall not include records related to claims audits. The Privacy Officer or designee shall have ultimate responsibility for determining what constitutes the designated record set.

The following information will <u>not</u> be considered part of the designated record set made available for inspection or copying. Requests for amendment to this information will be denied:

a. Psychotherapy notes.
b. Copies of health information kept in multiple locations - only the original should be included in the designated record set.
c. Information compiled in anticipation of, or for use in, a civil, criminal or administrative action or proceeding.
d. PHI that was obtained under a promise of confidentiality (other than from a health care provider), where the access requested would be reasonably likely to reveal the source of the information.
e. Quality improvement or risk management records.
f. Research documentation while a clinical trial is taking place, if the individual who is part of the clinical trial agreed to denial of access upon participation.

g. Appointment schedules.
h. Information compiled in anticipation of a government or administrative proceeding.
i. Cancer registry information.

1. A request must be in writing, provide a reason for the request and be mailed to the following address:

   Privacy Officer
   (Address)
   (Telephone number)

2. **Timing of Decision.** The Trust will act on the request within 60 days of receipt of the request. The Trust may extend the time to comply by 30 days, provided that the insurer or the administrator notifies the individual in writing within the first 60 days and explains the reasons for the delay and the date by which the Trust will act.

3. **Reason for Denial.** The Trust will deny the request for amendment if the Privacy Officer determines that the PHI or other record:

   a. Was not created by the Trust, unless the individual provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the request,
   b. Is not part of the designated record set,
   c. Is not available for inspection under HIPAA (pursuant to the Trust's Policy for Rights of Access to PHI), or
   d. Is accurate and complete.

4. **Accepting the Amendment.** If the Trust accepts the request for the amendment in whole or in part, then the Trust will do the following:

   a. Make the appropriate amendment to PHI by providing a link to the affected records or appending the affected records within 60 days of the receipt of the request,

      NOTE: The privacy rules do not require that the Trust delete or expunge any PHI from its records. The Trust can simply provide a link within the affected document to the amendment. Also, individuals requesting an amendment have no right under the privacy rule to determine the content of any amendment that is made. Individuals do not have the right to make the actual changes to their PHI. It is within the Trust's discretion to make the appropriate amendment.

   b. Within 60 days of the receipt of the request, inform the individual of the amendment that will be made and obtain from the individual the identification of and an agreement to have the insurer or the administrator notify persons who should be aware of the amendment.

   c. Make reasonable efforts to provide the amendment to persons identified by the individual or persons, including Business Associates, which the insurer or the administrator knows may have or could rely on the PHI to the detriment of the individual.

5. **Denying the Amendment.** If the request to amend is denied, in whole or in part, then the Privacy Officer or designee will provide a denial notice containing the following information:

   a. Basis for denial,
   b. A statement of the individual's right to submit a statement of disagreement with the denial, and how this statement can be filed,
   c. A statement that if an individual does not submit a statement of disagreement, the individual has a right to request that the Trust furnish a copy of the Request for Amendment and Denial of the request with future disclosures of the PHI that was the subject of the request, and
   d. A description of how an individual can file a complaint with the Trust and the U.S. Department of Health and Human Services.

6. **Statement of Disagreement** Where the request to amend is denied, the individual may submit a

written statement disagreeing with the denial and explaining the basis for the disagreement. Such a statement cannot exceed 2 pages.

7. **Rebuttal Statement.** The Trust, through its Privacy Officer, may then issue a written rebuttal to the individual's statement of disagreement. If the Trust prepares a rebuttal statement, a copy of the rebuttal will be provided to the individual who submitted the statement of disagreement.

8. **Recordkeeping**. The request for amendment, the denial, any statement of disagreement and any rebuttal statement will be linked or appended to the related PHI kept in the designated record set.

9. **Future Disclosures**

   a. If a statement of disagreement has been submitted, the statement or a summary of the statement will be attached to any subsequent disclosure of the PHI.
   b. If a statement of disagreement has not been submitted, then the Trust will (upon the individual's request) include the individual's request for amendment and the denial (or a summary of this information) with any subsequent disclosure of the PHI.
   c. When a subsequent disclosure is made in the form of an electronic transmission that is a standard transaction under HIPAA's Electronic Data Interchange ("EDI") rules, the required information will be sent separately to the recipient of the information, if the transaction does not permit the additional material to be included with the disclosure.

10. **Action on Amendment Made By Other Covered Entities.** Upon notification of an amendment to PHI by another covered entity (e.g. another health plan or medical provider), the Trust will amend the PHI in its designated record set.

11. **Documentation.** The Trust will document the designated record set that is subject to access by individuals. It will also document the title of the individual responsible for receiving and processing requests for access by individuals. The Trust will also maintain any communication required by this procedure to be in writing (e.g. notice of denial).

RIGHT TO AMEND PHI FORMS

REQUEST TO AMEND PROTECTED HEALTH INFORMATION FORM

Individuals should use this form to request an amendment to PHI.

DENIAL OF REQUEST TO AMEND PROTECTED HEALTH INFORMATION FORM

The Privacy Officer should use this form to:

- Notify the individual of the denial of the Request to Amend PHI, and
- Provide a statement of the individual's right to have the denial reviewed.

STATEMENT DISAGREEING WITH DENIAL OF REQUEST TO AMEND PHI

Individuals should use this form to provide a written statement disagreeing with the denial of a request to amend PHI.

REBUTTAL TO STATEMENT DISAGREEING WITH DENIAL OF REQUEST TO AMEND PHI

The Privacy Officer should use this form to rebut the individual's statement disagreeing with the denial of a request to amend PHI.

ACCEPTANCE OF REQUEST TO AMEND PHI FORM

The Privacy Officer should use this form to advise the individual that their PHI has been amended and state the exact form of the amendment.

REQUEST TO AMEND PHI FORM
(Sample Form)

Date: _____

Name of Individual: _____

Address: _____

Social Security Number _____

I am requesting that an amendment be made to my PHI for the following reason:

_____

_____

_____

_____

_____

_____

Signature of Individual requesting PHI amendment: _____

Signature of Personal Representative
acting on behalf of the Individual, if the-Individual
is not making the Request for Privacy Protection: _____

DENIAL OF REQUEST TO AMEND PHI FORM
(Sample Form)

Date: _____

Date of Request to Amend Protected Health Information (PHI): _____

Name of Individual Requesting PHI Amendment: _____

Your Request to Amend your PHI has been denied for the following reasons:

- ❑ The Trust did not create the information, which is the subject of your request to amend. Please contact the originator of the health information to act upon your request. According to our records the originator is:
  _____

- ❑ The information that is the subject of your request to amend is accurate and complete.

- ❑ The information that is the subject of your request to amend is not a part of the record you requested be amended.

- ❑ The information that is the subject of your request to amend includes information you are not permitted by law to change because it involves
  _____

  _____

You have the right to submit to the Trust a written statement (no longer than 2 pages) describing why you disagree with this denial. This statement can be sent to the Privacy Officer at the address listed in the attached privacy notice. The Trust then may prepare a written rebuttal to your statement of disagreement. The Trust is not obligated to prepare this statement, but if the Trust prepares a rebuttal it will provide you with a copy. If you elect to file a statement of disagreement, the Trust will append your request for amendment, the Trust's denial, your statement of disagreement, and any rebuttal statement to any future disclosure of the PHI that is the subject of the request.

If you choose not to submit a statement of disagreement, you may request (by sending a letter to the Privacy Officer) that the Trust provide your request for amendment and the Trust's denial with any future disclosure of the PHI that is the subject of the request.

You have the right to file a Complaint with the Trust or the Secretary of the U.S. Department of Health and Human Services, as outlined in the attached copy of the Trust's Privacy Notice.

Telephone # of Privacy Officer: _____

Signature of Privacy Officer: _____

STATEMENT DISAGREEING WITH DENIAL OF REQUEST TO AMEND PHI
(Sample Form)

Name of Individual: _____

Date: _____

I disagree with the denial of my request to amend my PHI for the following reasons:

_____

_____

_____

_____

_____

_____

_____

_____

Signature of Individual submitting Statement of Disagreement with Denial of Request to Amend PHI:

_____

Signature of Personal Representative acting on behalf of the Individual, if the Individual is not making the Statement Disagreeing with Denial of Request to Amend PHI:

_____

REBUTTAL TO STATEMENT DISAGREEING WITH DENIAL OF REQUEST TO AMEND PHI
(Sample Form)

Name of Individual: _____

Date: _____

The following represents a rebuttal to the individual's Statement Disagreeing with Denial of Request to Amend PHI:

_____

_____

_____

_____

_____

_____

_____

_____

Signature of Privacy Officer: _____

ACCEPTANCE OF REQUEST TO AMEND PHI FORM
(Sample Form)

Name of Individual: _____

Date: _____

Your request to amend your health information was received the by the Trust on _____.

Your request has been granted and your health information has been amended as follows:

_____

_____

_____

_____

_____

_____

_____

_____

The Trust will provide the amended information to any individual or entity that you request receive it by providing the Privacy Officer with a written request to do so and the name and address of any individual or entity that you wish to receive the amended health information.

If The Trust is aware of any Business Associates of the Trust who have the disputed health information and who need the amended information for your benefit, the Trust will provide the amended information to them.

Signature of Privacy Officer: _____

14. RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI

14.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.528 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI POLICY

1. A covered individual has the right to request and receive an accounting of disclosures of that individual's PHI made by the Trust in the six years before the date of the request, including the following disclosures:

    a. Uses and disclosures not according to policy by a workforce member or Business Associate,
    b. Disclosures that do not require an authorization under the Trust's Policy for Disclosure of PHI for Public Health, Law Enforcement or Legal Process, and
    c. Federal and state mandated disclosures.

2. The following disclosures need not be accounted for:

    a. Disclosures of PHI for treatment, payment or health care operations,
    b. Disclosures to the covered individual,
    c. Disclosures for national security or intelligence purposes,
    d. Disclosures to correctional institutions or law enforcement officer having lawful custody of an inmate as provided under the privacy rules,
    e. Disclosures before the compliance date of the privacy rule (April 14, 2004),
    f. Disclosures made pursuant to a valid authorization,
    g. Disclosures incident to a use or disclosure otherwise permitted or required by HIPAA,
    h. Disclosures that are part of a "limited data set" as described in section 164.514(e) of the privacy rules,
    i. Disclosures for facilities directories or to persons involved in the individual's care or other notification purposes.

14.2 PROCEDURES

ACCOUNTING REQUEST FORM

1. An individual who requests an accounting must use the form entitled Individual Request for Accounting of Disclosures of Protected Health Information ("Accounting Request Form").

2. The Privacy Officer will provide an Accounting Request Form to any individual who wishes to request an accounting of disclosures.

3. The Accounting Request Form must be completed and signed by the individual. The individual may mail, fax or deliver the Accounting Request Form to the Privacy Officer at the following address:

    Privacy Officer
    (Address)
    (Telephone number)
    (Fax number)

RESPONSE TO REQUEST

1. The Privacy Officer or delegate of the Privacy Officer will review the Accounting Request Form and prepare a written accounting of all uses and disclosures for which an accounting is required under the Trust's Right to Accounting Policy.

2. The Privacy Officer will respond as follows:

a. An accounting will be provided within sixty days of receipt of the Request for Accounting Form by the Privacy Officer.

b. If the insurer or the administrator are unable to provide the accounting within 60 days, The Trust will invoke one thirty-day extension, provided the individual is notified by the Privacy Officer in writing within the first 60 days of the reason for the delay and the date by which the Trust will provide the accounting.

c. Upon request, one accounting for an individual in a twelve-month period will be provided without charge. The Trust will impose a fee based on labor and supplies for each additional request during the twelve-month period. However, the Privacy Officer will notify the individual of the fee in advance and allow the individual to modify or withdraw the request.

EXCEPTIONS FROM THE ACCOUNTING REQUIREMENT

1. The accounting requirement does not apply to disclosures set out in section 2 of the Trust's Right to Accounting Policy.

2. In addition, the Trust must temporarily suspend the individual's right to receive an accounting of such uses and disclosures to a health oversight agency ("agency') or law enforcement officer ("officer") if a temporary suspension is requested by the agency or officer in accordance with the following procedures:

   a. The agency or officer states in writing to the insurer or the administrator that providing such accounting to the individual would be reasonably likely to impede the agency's activities and specifies the period of time for which the suspension of the right to an accounting of these disclosures is required, or

   b. The agency or officer orally states to the insurer or the administrator that providing such accounting to the individual would be reasonably likely to impede the agency's activities and specifies the period of time for the suspension. The insurer or the administrator must document the statement (including the identity of the agency or officer making the statement) and must limit the temporary suspension to no longer than 30 days from the date of the oral statement (unless a written statement complying with the requirements of paragraph (a) is submitted).

INFORMATION TO BE PROVIDED IN AN ACCOUNTING

1. With the exception of uses and disclosures of PHI that are not subject to an accounting in accordance with the Trust's Right to Accounting Policy, the Trust must include in an accounting any uses and disclosures of PHI made during the six years before the date of the accounting (or fewer years if the Trust's HIPAA compliance date is fewer than six years before the accounting).

2. Disclosures made to or by Business Associates of the Trust must be included in the accounting unless it falls into one of the exceptions for the right to an accounting.

3. For each disclosure, the accounting must include:

   a. The date of the disclosure,

   b. The name of the entity or person who received the PHI and, if known, the address of the entity or person,

   c. A brief description of the PHI disclosed, and

   d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written, request for disclosure, if any.

4. To the extent that the Trust has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting regarding this multiple disclosure may provide:

    a. All information that would be otherwise required for the first disclosure in the accounting period,

    b. The frequency, periodicity or number of disclosures made during the accounting period, and

    c. The date of the last such disclosure in the accounting period.

DOCUMENTATION

The Trust will keep any information that is the subject of an accounting and any written accounting according to its Record Retention policy.

REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORMS

REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM

Individuals should use this form to request an accounting of disclosures of PHI.

ACCOUNTING OF DISCLOSURES OF PHI FORM

The Privacy Officer should use this form to disclose PHI disclosures that do not fall within the exceptions allowed under the privacy rules.

DENIAL OF REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM

The Privacy Officer should use this form to:

- Notify the individual of the denial of the request for an accounting of PHI disclosures, and
- Provide a statement of the individual's right to have the denial reviewed

REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM
(Sample Form)

Date: _____

Name of Individual: _____

Address: _____

Social Security Number:_____

I am requesting an accounting of disclosures of my PHI for the following time period:

_____

(Note: The Trust will provide an accounting for disclosure for a period of six years or less, but only for disclosures made after April 14, 2004).

I understand that the accounting will not include disclosures for which an accounting is not required under the HIPAA privacy rules and under the Trust's Right to Accounting of Disclosures of PHI Policy. I also understand that where the Trust provides an accounting to me, it will provide it once free-of-charge within a twelve month period. Any additional request for an accounting within the 12-month period will be subject to a reasonable cost-based fee.

Signature of Individual Requesting Accounting of Disclosures of PHI:

_____

Signature of Personal Representative acting on behalf of the Individual, if the Individual is not making the Request for Accounting of Disclosures of PHI:

_____

ACCOUNTING FOR DISCLOSURES OF PHI FORM
(Sample Form)

Date: _____

Name of Individual: _____

The following disclosures of your Protected Health Information have been made by the Trust.

DISCLOSURE

Date of the disclosure: _____

Name of the entity or person who received the PHI:
_____

Address of the entity or person who received the PHI:
_____

Description of the PHI disclosed:
_____

_____

Purpose of the disclosure:
_____

_____

For multiple similar disclosures, the frequency or number of disclosures and date of last disclosure:

_____

DISCLOSURE

Date of the disclosure: _____

Name of the entity or person who received the PHI:
_____

Address of the entity or person who received the PHI:

_____

Description of the PHI disclosed:

_____

_____

Purpose of the disclosure:
_____

_____

For multiple similar disclosures, the frequency or number of disclosures and date of last disclosure:

_____

Signature of Privacy Officer: _____

DENIAL OF REQUEST FOR ACCOUNTING OF DISCLOSURES OF PHI FORM
(Sample Form)

Date: _____

Date of Request for Accounting of Disclosures of PHI: _____

Name of Individual Requesting Accounting of PHI Disclosures: _____

Your request for an Accounting of Disclosures of PHI has been denied for the following reasons:

_____

_____

_____

_____

Name of Privacy Officer: _____

Signature of Privacy Officer: _____

15. DISTRIBUTION OF PRIVACY NOTICE

15.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.520 of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

DISTRIBUTION OF PRIVACY NOTICE POLICY

The Trust will prepare and distribute a Privacy Notice describing the Trust's privacy policies and procedures. The Notice will be provided by mail to a covered individual at the following times:

- Upon request,
- No later than April 14, 2004 to all Trust participants,
- To all new Trust participants at the time of enrollment, and
- Within 60 days of a material revision in the Privacy Notice

15.2 PROCEDURES

1. Before April 14, 2004, the Trust will mail the Trust's Privacy Notice to all Trust participants as of the date of mailing.

2. The Trust will include a Privacy Notice in new participant enrollment packets to ensure that newly covered plan participants receive a copy of the Notice.

3. Once every three years, the Privacy Officer will notify all Trust participants that the Privacy Notice is available.

4. Whenever there is a material revision to the Privacy Notice, a copy will be mailed by the Privacy Officer to all Trust participants within 60 days of the revision.

5. If the Trust maintains a web site that provides information about the Trust's benefits or customer services, then the Privacy Officer will ensure that the Privacy Notice is prominently posted and available on the web site.

6. The Privacy Officer will maintain a copy of the Privacy Notice and any revised Notices according to the Trust's Record Retention Policy.

NOTICE OF PRIVACY PRACTICES

Purpose of This Notice and Effective Date

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.

Effective date. The effective date of this Notice is April 14, 2003.

This Notice is required by law. The Tongass Timber Trust ("TTT") is required by law to take reasonable steps to ensure the privacy of your personally identifiable health information and to inform you about:

1. TTT's uses and disclosures of Protected Health Information (PHI),
2. Your rights to privacy with respect to your PHI,
3. TTT's duties with respect to your PHI,
4. Your right to file a complaint with TTT and with the Secretary of the United States Department of Health and Human Services (HHS), and
5. The person or office you should contact for further information about TTT's privacy practices.

Your Protected Health Information

What is Protected Health Information (PHI)?

The term "Protected Health Information" (PHI) includes all individually identifiable health information related to your past, present or future physical or mental health condition or to payment for health care. PHI includes information maintained by TTT in oral, written, or electronic form.

When Can TTT Disclose Your PHI Without Your Authorization?

Under the law, TTT may disclose your PHI without your consent or authorization, or the opportunity to agree or object, in the following cases:

◆*At your request.* If you request it, TTT is required to give you access to certain PHI in order to allow you to inspect and/or copy it.
◆*As required by HHS.* The Secretary of the United States Department of Health and Human Services may require the disclosure of your PHI to investigate or determine the TTT's compliance with the privacy regulations.
◆*For treatment, payment or health care operations.* TTT and its business associates will use PHI in order to carry out:

- ➲Treatment,
- ➲Payment, or
- ➲Health care operations.

Treatment is the provision, coordination, or management of health care and related services. It also includes but is not limited to consultations and referrals between one or more of your providers.

Payment includes but is not limited to actions to make coverage determinations and payment (including billing, claims management, subrogation, plan reimbursement, reviews for medical necessity and appropriateness of care and utilization review and preauthorizations).

Health care operations includes but is not limited to quality assessment and improvement, reviewing competence or qualifications of health care professionals, underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts. It also includes disease

management, case management, conducting or arranging for medical review, legal services, and auditing functions including fraud and abuse compliance programs, business planning and development, business management and general administrative activities.

Disclosure to your group health plan's Plan Sponsor. TTT will also disclose PHI to the Plan Sponsor of your group health plan for purposes related to treatment, payment, and health care operations, if the Plan Sponsor has adopted amendments to its Plan Documents to permit this use and disclosure as required by federal law. For example, TTT may disclose information to the Plan Sponsor to allow it to decide an appeal or review of an eligibility question or a subrogation claim.

When Does the Disclosure of Your PHI Require Your Written Authorization?

Except as otherwise indicated in this Notice, uses and disclosures will be made only with your written authorization subject to your right to revoke your authorization.

When Is the Use or Disclosure of My PHI Permitted and My Consent, Authorization or Opportunity to Object Is Not Required?

TTT is allowed under federal law to use and disclose your PHI without your consent or authorization under the following circumstances:

1. *When required by applicable law.*
2. *Public health purposes.*
3. *Domestic violence or abuse situations.*
4. *Health oversight activities.*
5. *Legal proceedings.*
6. *Law enforcement health purposes.*
7. *Law enforcement emergency purposes.*
8. *Determining cause of death and organ donation.*
9. *Funeral purposes.*
10. *Research.*
11. *Health or safety threats.*
12. *Workers' compensation programs.*

Are there Other Uses or Disclosures?

TTT may contact you to provide you information about treatment alternatives or other health-related benefits and services that may be of interest to you.

TTT may disclose protected health information to your group health plan sponsor for reviewing your appeal of a benefit claim or for other reasons regarding the administration of TTT or your employer's group health plan.

Your Individual Privacy Rights

Can I Request Restrictions on Uses and Disclosures of my PHI?

You may request TTT to:

1. Restrict the uses and disclosures of your PHI to carry out treatment, payment or health care operations, or

2. Restrict uses and disclosures to family members, relatives, friends or other persons identified by you who are involved in your care.

TTT, however, is not required to agree to your request if TTT determines your request to be unreasonable.

Make such requests in writing to: The TTT Privacy Contact Person who is _____. He/She can be contacted at _____, _____.

Can I Request Confidential Communications?

TTT will accommodate an individual's reasonable request to receive communications of PHI by alternative means or at alternative locations where the request includes a statement that disclosure could endanger the individual.

You or your personal representative will be required to complete a form to request restrictions on uses and disclosures of your PHI. Make such requests to the Privacy Contact Person, listed above.

Can I Inspect and Copy My PHI?

You have a right to inspect and obtain a copy of your PHI for as long as TTT maintains the PHI.

TTT must provide the requested information within 30 days if the information is maintained on site or within 60 days if the information is maintained offsite. A single 30-day extension is allowed if TTT is unable to comply with the deadline.

You or your personal representative will be required to complete a form to request access to the PHI. A reasonable fee may be charged. Requests for access to PHI should be made to the Privacy Contact Person, listed above.

If access is denied, you or your personal representative will be provided with a written denial setting forth the basis for the denial, a description of how you may exercise your review rights and a description of how you may complain to the Plan and HHS.

Do I Have the Right to Amend My PHI?

You have the right to request that TTT amend your PHI or a record about you for as long as the PHI is maintained subject to certain exceptions.

TTT has 60 days after receiving your request to act on it. TTT is allowed a single 30-day extension if TTT is unable to comply with the 60-day deadline. If TTT denied your request in whole or part, TTT must provide you with a written denial that explains the basis for the decision. You or your personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosures of that PHI.

You should make your request to amend PHI to the Privacy Contact Person, listed above.

You or your personal representative will be required to complete a written form to amendment of the PHI and include a reason to support the requested amendment.

Do I Have the Right to Receive an Accounting of TTT's Disclosures of My PHI?

At your request, TTT will also provide you with an accounting of certain disclosures by TTT of your PHI. TTT is not required to provide you with an accounting of disclosures related to treatment, payment, or health care operations, or disclosures made to you or authorized by you in writing.

TTT has 60 days to provide the accounting. TTT is allowed an additional 30 days if TTT gives you a written statement of the reasons for the delay and the date by which the accounting will be provided.

If you request more than one accounting within a 12-month period, TTT will charge a reasonable fee for each subsequent accounting.

Do I Have the Right to Receive a Paper Copy of This Notice Upon Request?

Yes. To obtain a paper copy of this Notice, contact the Privacy Contact Person, listed above.

Can My Personal Representative Act on My behalf Regarding My Privacy Rights?

You may exercise your rights through a personal representative. Your personal representative will be required to produce evidence of authority to act on your behalf before the personal representative will be given access to your PHI or be allowed to take any action for you. Proof of such authority will be a completed, signed and approved Appointment of Personal Representative form. You may obtain this form by calling the TTT Administration Office.

TTT retains discretion to deny access to your PHI to a personal representative to provide protection to those vulnerable people who depend on others to exercise their rights under these rules and who may be subject to abuse or neglect.

TTT will recognize certain individuals as personal representatives without you having to complete an Appointment of Personal Representative form. For example, TTT will automatically consider a spouse to be the personal representative of an individual covered by a group health plan. In addition, TTT will consider a parent or guardian as the personal representative of an unemancipated minor unless applicable law requires otherwise. A spouse or a parent may act on an individual's behalf, including requesting access to their PHI. Spouses and unemancipated minors may, however, request that TTT restrict information that goes to family members.

TTT's Duties Regarding Privacy

Maintaining Your Privacy

TTT is required by law to maintain the privacy of your PHI and to provide you and your eligible dependents with notice of its legal duties and privacy practices.

This Notice is effective beginning on April 14, 2004 and TTT is required to comply with the terms of this Notice. However, TTT reserves the right to change its privacy practices and to apply the changes to any PHI received or maintained by TTT prior to that date. If a privacy practice is changed, a revised version of this Notice will be provided to you and to all past and present participants and beneficiaries for whom TTT still maintains PHI via mail.

Any revised version of this Notice will be distributed within 60 days of the effective date of any material change to:

- The uses or disclosures of PHI,
- Your individual rights,
- The duties of TTT, or
- Other privacy practices stated in this notice.

Disclosing Only the Minimum Necessary Protected Health Information

When using or disclosing PHI or when requesting PHI from another covered entity, TTT will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations.

However, the minimum necessary standard will not apply in the following situations:

- Disclosures to or requests by a health care provider for treatment,
- Uses or disclosures made to you,
- Disclosures made to the Secretary of the United States Department of Health and Human Services pursuant to its enforcement activities under HIPAA,
- Uses or disclosures required by law, and
- Uses or disclosures required for TTT's compliance with the HIPAA privacy regulations.

This Notice does not apply to information that has been de-identified. De-identified information is information that:

- Does not identify you, and
- With respect to which there is no reasonable basis to believe that the information can be used to identify you.

In addition, TTT may use or disclose "summary health information" to your group health plan's Plan Sponsor for obtaining premium bids or modifying, amending or terminating the group health plan. Summary information summarizes the claims history, claims expenses or type of claims experienced by individuals for whom a Plan Sponsor has provided health benefits under a group health plan. Identifying information will be deleted from summary health information, in accordance with HIPAA.

Your Right to File a Complaint with TTT or the HHS Secretary

If you believe that your privacy rights have been violated, you may file a complaint with TTT in care of the following individual:

Privacy Official

_____
_____
_____
_____

You may also file a complaint with:

Secretary of the U.S. Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue S.W.
Washington, D.C. 20201

TTT will not retaliate against you for filing a complaint.

If You Need More Information

If you have any questions regarding this notice or the subjects addressed in it, you may contact the following individual at the TTT Administrative Office:

Privacy Contact Person

_____
_____
_____
_____

Conclusion

The federal Health Insurance Portability and Accountability Act, known as HIPAA, regulate PHI use and disclosure by TTT. You may find these rules at 45 *Code of Federal Regulations* Parts 160 and 164. This Notice attempts to summarize the regulations. The regulations will supersede this Notice if there is any discrepancy between the information in this Notice and the regulations.

16. TRAINING

16.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(b) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

TRAINING POLICY

It is the policy of the Trust that the administrator and the insurer train their own staff on all Trust policies and procedures concerning the use or disclosure of protected health information implemented for compliance with the privacy requirements under HIPAA.

16.2 PROCEDURES

1. **Timing of Training:**

   a. The insurer and the administrator will provide training to all of their personnel no later than April 14, 2003.

   b. After April 14, 2003, each new employee of the insurer and the administrator will be trained within a reasonable time after they join the office.

   c. Training will also be provided to each employee of the insurer and the administrator whose functions are affected by a material change in the Trust's policies and procedures. This training will take place within a reasonable time after the material change in policy or procedure becomes effective.

   d. The insurer and the administrator will re-train personnel as necessary.

   e. The insurer and the administrator will train temporary employees and independent contractors as necessary based on their assignment.

2. **Documentation:**

   Each employee of the insurer and the administrator must certify that they have completed the initial privacy training. They must also certify their participation in any subsequent training.

3. **Business Associates:**

   It shall be the responsibility of each of the Trust's Business Associates to train its own workforce.

17. COMPLAINTS FOR VIOLATION OF PRIVACY RULES

17.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(d) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

COMPLAINT POLICY

The Trust accepts and will investigate complaints of violations of the Trust's privacy policies and procedures from covered individuals as well as complaints from the insurer.

The Privacy Officer or designee will determine:

- Whether there has been a violation of the Trust's privacy policies and procedures,
- The seriousness and effect of the violation, and
- Any corrective action that may be taken

The Privacy Officer or designee will document all complaints received and their outcome, if any.

17.2 PROCEDURES

FORM OF COMPLAINTS

1. Complaints must be in writing. They may be on the Trust's Complaint Form or they may be in another written form. Complaints must contain:

    a. The date of the complaint,
    b. The date of the alleged violation or other action that is the subject of the complaint,
    c. The name or position of the party against whom the complaint is made,
    d. The substance of the complaint, and
    e. The name and signature of the complainant.

2. The Privacy Officer will accept written complaints from covered individuals and from the insurer. When the insurer or the administrator receive oral complaints from covered individuals, they will inform the individual that complaints must be in writing and they will send the individual a complaint form to complete and return to the Privacy Officer.

3. The insurer will forward any written complaints it receives to the Privacy Officer for review.

4. The administrator will date-stamp 'the complaint when it is received.

DISPOSITION OF COMPLAINT

3. The Privacy Officer will:

    a. Investigate the complaint,
    b. Question the covered individual or employee making the complaint, if necessary,
    c. Question the party alleged to have violated the privacy policies and procedures,
    d. Consider any documents, evidence or testimony offered on behalf of the party alleged to have violated the Trust's privacy policies and procedures,
    e. Determine whether there has been a violation of the Trust's privacy policies and procedures,
    f. Determine whether any corrective action is necessary as a result of the complaint,
    g. Implement any corrective measures necessary as a result of the complaint
    h. Document any corrective measures taken,
    i. When appropriate, inform the employee, participant or beneficiary of the determinations made

with regard to the complaint,

j. Make and keep a record of the complaint investigation, including the complaint and the Trust's findings, to ensure consistency of determinations and corrective measures for similar violations, and

k. Retain written records for six years beginning from the date on which there is a disposition of the complaint.

6. The Privacy Officer will make a disposition of the complaint.

COMPLAINT FORM
(Sample Form)

Name of Complainant: _____

Current Date: _____

Date of Violation: _____

Patient Name, if applicable: _____

Patient's relationship to Plan Participant: _____

Name of Employee perceived to have violated the privacy policies and procedures:

_____

My complaint is: _____

_____

_____

_____

_____

_____

_____

_____

I am completing this complaint form in regard to the Trust's practices, policies, procedures or compliance under the privacy standards of the Health Insurance Portability and Accountability Act (HIPAA). I understand that although The Trust reviews and makes determinations regarding every complaint received, the Trust does not respond to every complaint in writing.

Signature of Complainant: _____

REPORT OF COMPLAINT INVESTIGATION FORM
(Sample Form)

Current Date: _____

Date of Incident: _____

Name of Complainant: _____

Name of Employee perceived to have violated the privacy policies and procedures:

_____

Report of Investigation of Complaint Regarding Violation of privacy policies and procedures:

_____

_____

_____

_____

_____

_____

_____

_____

Corrective measures, if any, and date of implementation: _____

_____

_____

Signature of Privacy Officer: _____

18. ANTI-RETALIATION

18.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(g) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ANTI-RETALIATION POLICY

In compliance with Section 164.530, the Trust will not take retaliatory action against any person who files a complaint with the Trust or with the U.S. Department of Health and Human Services.

The Trust will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for exercising their rights under the privacy rules or for filing a complaint or participating in any other process established by the privacy rules; or

2. Any individual or other person or entity for filing a complaint about the Trust's HIPAA privacy compliance with the Secretary of Health and Human Services; or

3. Any individual or other person or entity for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing involving the Trust's HIPAA privacy policies and procedures; or

4. Any individual or other person or entity for opposing any act or practice made unlawful by HIPAA, provided the individual or person or entity has a good faith belief that the practice opposed is unlawful. The manner of the opposition must be reasonable and not involve a disclosure of PHI in violation of HIPAA regulations.

19. MITIGATION OF HARMFUL EFFECTS

19.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(f) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

MITIGATION OF HARMFUL EFFECTS POLICY

The Trust will mitigate to the extent practicable any harmful effects known to the insurer or the administrator by a use or disclosure of protected health information (PHI) in violation of the Trust's policies and procedures or HIPAA regulations by employees of the insurer, the administrator, or any Business Associate.

The Trust must be advised of or otherwise made aware of any use or disclosure that violates the Trust's procedures and/or HIPAA in order to be able to mitigate harmful effects. In order for the Trust to take appropriate action in mitigation of harmful effects, the Privacy Officer must have been informed in writing of the violation by an individual or a Business Associate. The Privacy Officer may also review complaints from a members of the insurer's or the administrator's workforces.

When mitigating harmful effects, the Trust will take reasonable steps based on knowledge of where the information has been disclosed, how it might be used to cause harm to an individual, and what steps can actually have a mitigating effect in that specific situation.

20. SANCTIONS FOR VIOLATION OF PRIVACY RULES

20.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(e) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

SANCTIONS POLICY

An employee of the insurer or the administrator who is responsible for handling Protected Health Information of covered individuals will be sanctioned for violating the HIPAA privacy rules and the privacy policies and procedures adopted by the Trust in accordance with the sanction policies of the insurer and the administrator.

The Privacy Officer will determine whether there has been a violation of the privacy rules, the seriousness and effect of the violation and the appropriateness and adequacy of the sanction to be imposed..

The Privacy Officer has discretion to determine appropriate sanctions for violation of the privacy rules. Sanctions undertaken or imposed directly by the insurer or the administrator will be taken into account by the Privacy Officer in determining the appropriateness of the sanction.

20.2 PROCEDURES

DETERMINATION OF VIOLATION

2. The insurer, the administrator, any Business Associates and Trustees are required to report any perceived violations of the Trust's privacy rules to the Privacy Officer. Reports must be made in writing.

3. The Privacy Officer will:

    a. Investigate the alleged violation of the privacy rules,
    b. Question the insurer or the administrator, Business Associate or Trustee reporting the perceived violation,
    c. Question the employee, Business Associate or Trustee who is alleged to have violated the privacy rules,
    d. Consider any evidence or testimony accompanying the report of violation or submitted on behalf of the employee alleged to have violated the privacy rules,
    e. Determine whether there has been a violation of the privacy rules; and
    f. Make and keep a record of the investigation.

DETERMATION OF SANCTION

4. The Privacy Officer will determine:

    a. The gravity of the violation of the privacy rules, and .
    b. The appropriate sanction to be imposed on the employee.

5. The Privacy Officer has discretion to determine appropriate sanctions and will consider:

    a. Whether the violation is accidental or egregious,
    b. Whether it is a first-time violation or a repeated violation, and
    c. Current human resources policies and practices governing other workplace sanctions.

3. The Trust will apply appropriate sanctions against any person with access to PHI who fails to comply with these Privacy Policies and Procedures and applicable law. The Trust may take one or more of the following steps depending on the severity and frequency of the offense:

a. Take whatever action is necessary to protect the confidentiality of all PHI.
b. Counsel the responsible party on the legal requirements for protection of PHI and the requirements of these Policies and Procedures.
c. Temporarily or permanently prevent the release of PHI to the responsible party.
d. Take steps in accordance with the Trust's governing documents to remove the responsible party.
e. Take steps in accordance with any applicable Business Associate Addendum or other service provider agreements to obtain redress against the responsible party.

4. The Privacy Officer will make and keep a record of sanctions imposed to ensure consistency of sanctions for similar violations.

5. Sanctions will not be imposed for disclosures of protected health information that meet the conditions set out in sections 164.530(g)(2) and 164.502(j) of the privacy rule regarding whistleblower protections.

REPORT OF PRIVACY RULES VIOLATION FORM
(Sample Form)

Current Date: _____

Date of Violation: _____

Name of Employee perceived to have violated the privacy rules:

_____

Employee Number, if applicable _____

Work location / firm name _____

Perceived violation of privacy rules: _____

_____

Name of Person completing this Report (please print): _____

Signature of Person completing this Report: _____

SANCTION FOR VIOLATION OF PRIVACY RULES FORM
(Sample Form)

Current Date: _____

Date of Violation: _____

Name of Employee found to have violated the privacy rules: _____

Employee Number, if applicable: _____

Firm Name: _____

Address: _____

Manager Name: _____

Sanction for violation of privacy rules: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Signature of Privacy Officer: _____

21. JOB DESCRIPTION FOR PRIVACY OFFICER

Position Title: Privacy Officer

Position Summary: The position of Privacy Officer is required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Officer is responsible for coordinating the TTT Timber Trust (the "Trust") policies and procedures under HIPAA's privacy rules and any applicable state law and monitoring and deciding any issues that occur under the rules and the Trust's privacy practices.

Reports to: The Privacy Officer reports to the Trustees of the Tongass Timber Trust.

Essential Functions:

The Privacy Officer is responsible for the following tasks:

1. Developing and implementing HIPAA's privacy rules as applicable to the Tongass Timber Trust, in coordination with the Trustee, consultants and legal counsel,

2. Developing training programs for the Trust's staff (if any), professional advisors, and Trustees and, where appropriate, contractors, Business Associates and other third parties,

3. Publishing and distributing the privacy notice,

4. Serving as the designated decision maker for issues and questions involving interpretation of the privacy rules, in coordination with the Trust Counsel,

5. Inventorying the uses and disclosures of all protected health information (PHI),

6. Ensuring that legal issues in drafting compliance documents are addressed, including amendment of Trust documents, negotiation of Business Associate contracts and development of authorizations,

7. Coordinating with contributing employers' functions such as FMLA leave, drug testing and fitness-for-duty examinations,

8. Developing and implementing appropriate firewalls between the employer and the Health Plan,

9. Tracking releases of PHI that are not for purposes of treatment, payment or operations, so that individuals may review or receive a report on such activities,

10. Establishing structures to ensure individual rights guaranteed by HIPAA,

11. Setting up a complaint process that provides for consistent application of sanctions for violation,

12. Developing overall privacy policies and procedures for the Trust as well as a notice of information practices and forms necessary to implement the Trust's policies,

13. Establishing programs to audit and monitor Business Associates and internal privacy compliance, including the performance of the initial and periodic privacy risk assessments,

14. Cooperating with the Office of Civil Rights or other applicable governmental agency in any compliance review or investigations, and

15. Keeping up to date on the latest privacy and security developments and federal and state laws and regulations.

Qualifications: The position requires the following minimum qualifications:

1. Minimum five years experience in the industry unless and owner or officer of a participating employer,
2. Familiarity with federal and state laws and regulations concerning information security and privacy,
3. Familiarity with federal and state laws governing Tongass Timber Trust,
4. Familiarity with the Tongass Timber Trust business functions and operational structure,
5. Ability to communicate both orally and in writing,
6. Strong interpersonal skills,
7. Strong organizational and problem-solving skills,
8. Ability to work in a team-oriented environment.

The Privacy Officer will be assisted by the Trust's professional advisors, including the Trust's legal Counsel and the Consultant.

22. MARKETING

22.1 POLICY STATEMENT & PROCEDURE

This policy and procedure is adopted pursuant to the sections 164.501 and 164.508(a)(3) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

MARKETING POLICY

It is the policy of the Tongass Timber Trust not to engage in marketing as that term is defined in the privacy rules under the Health Insurance Portability and Accountability Act of 1996.

The following activities are not marketing, and therefore can be done without the Trust obtaining an individual authorization:

a. A communication describing a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of the Trust, including communications about the entities participating in the health plan's network; replacement of, or enhancements to the health plan; and health-related products or services available only to a participant that add value to, but are not part of, the health plan's benefits.

b. A communication made for treatment of the individual;

c. A communication for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, providers, or settings of care to the individual;

23. RECORD RETENTION

23.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to various requirements of the privacy rules, including but not limited to Section 164.530(j), under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and general rules under the Employee Retirement Income Security Act of 1974 (ERISA).

RECORD RETENTION POLICY

This policy specifically focuses on the record retention period requirements specific to the administration of the Trust, and, as such, is not meant as an exhaustive list of all record retention requirements to which the Trust and/or an Employer may be subject under Federal laws other than the Employee Retirement Income Security Act of 1974 (ERISA) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

ERISA ERISA generally requires that the Trust maintain copies of all source documents and certain records for six years. Documents from which federal filings are made (including vouchers, worksheets, receipts, and resolutions) must be retained at least six years after the filing. Items such as detailed records of compensation and contributions that would be required to support individual participant eligibility and benefits under the Trust should be maintained indefinitely.

HIPAA Privacy HIPAA's privacy rules require that any required documentation must be retained -either in written or electronic form - for six years from either the date it was created or the date it was last in effect, whichever later. The Department of Labor (DOL) has established proposed ERISA guidelines for employee benefit plan administrators that wish to retain documents electronically. The Trust generally will follow the technology-neutral guidelines when retaining electronic records to show a good faith attempt to comply with HIPAA's recordkeeping provisions. Records that will be retained under the privacy rules, include, but are not limited to, plan documents, policies on PHI uses and disclosures, signed authorization forms, the privacy notice, documentation regarding individual rights and records, and business associate contracts.

23.2 PROCEDURES

1. General Files	Retention Period
General Correspondence	Current year plus two prior years
Claim Forms	Current year plus six prior years
Eligibility Records	Current year plus six prior years
Enrollment Forms	Current year plus six prior years
Employer Correspondence	Current year plus two prior years
Correspondence relating to claims and appeals	Current year plus two prior years

2. Accounting Records	Retention Period
Employer remittance reports	Current year plus six prior years and indefinitely if related to participant pension credits
General books of account	Current year plus six prior years
Cash receipts and disbursements ledgers	Current year plus six prior years
Bank deposit slips and statements	Current year plus six prior years
ERISA filings (5500, Summary Annual Reports, etc.)	Current year plus six prior years
Annual Plan audit	Current year plus six prior years

3. Administration Records	Retention Period
Original and subsequent Trust Agreements and any amendments	Retain permanently in chronological files
Original and subsequent Plan documents (rules and regulations) and any amendments	Retain permanently in chronological files
Insurance policies and riders, meeting minutes, annual reports, actuarial valuations, pertinent portions of collective bargaining agreements, IRS and Department of Labor filings (Form 5300, etc.)	Retain permanently in chronological files
Documents regarding decisions or policies related to the investment of Plan assets	Retain permanently in chronological files
Signed agreements, retainer or otherwise, related to all service providers	Retain permanently in chronological files
Supporting documentation and results of testing the Plan's nondiscrimination and top-heavy status	Retain for current year plus six prior years, although results of nondiscrimination testing must be updated at least every three years

4. HIPAA Records	Retention Period
Plan documents	Current year plus six prior years
Policies on PHI used and disclosures	Current year plus six prior years
Minimum necessary policies and procedures, including protocols for PHI use, routine disclosures and requests	Current year plus six prior years
All signed authorizations	Current year plus six prior years
The privacy notice	Current year plus six prior years
Documentation regarding the following individual rights: 1. Any communication that is required to be in writing (for example, a notice of denial of access); 2. Designated record sets subject to inspection and copying by an individual, and the name or title of the persons or offices responsible for receiving and processing the requests; 3. The name or title of the persons or offices responsible for receiving and processing individual requests for PHI amendments; and 4. Documentation of any agreed upon restrictions on the PHI use or disclosure requested by an individual	Current year plus six prior years
Records of PHI disclosure for non-TPO purposes	Current year plus six prior years
All individual complaints and their outcome	Current year plus six prior years
Records of any sanctions imposed on employees, agents, subcontractors or business associates	Current year plus six prior years
Records on any PHI use and disclosure for research purposes, as allowed without authorization under the privacy rules	Current year plus six prior years
Information on whether an entity is a hybrid or affiliated entity or an organized healthcare arrangement	Current year plus six prior years
Business associate contracts	Current year plus six prior years
Employee training manuals and procedures	Current year plus six prior years

Form of Record Retention • **Electronic Recordkeeping**	
ERISA	Under Department of Labor regulations, electronic media may be used provided: 1. The recordkeeping system reasonably ensures the integrity, accuracy, authenticity, and reliability of electronic records; 2. The electronic records are kept in a safe and accessible place, and may be readily inspected or examined; 3. The electronic records can be converted into paper copy; and 4. There are adequate records of management practices.
HIPAA Privacy	Use ERISA electronic recordkeeping rules until HIPAA rules for electronic recordkeeping have been finalized.

24. ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS

24.1 POLICY STATEMENT

This policy and procedure is adopted pursuant to Section 164.530(c) of the privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS POLICY

The insurer and the administrator will establish appropriate procedures for administrative, technical and physical safeguards to insure the security of PHI and prohibit access to PHI by anyone other than those individuals specifically authorized to work with PHI as part of the Trust operations.

24.2 PROCEDURES

The insurer and the administrator will adhere to the following security procedures to the extent applicable:

1. Email Policy: Email shall be used for appropriate business purposes.

2. Security Protocols: The insurer and the administrator will designate security protocols for electronic or paper, documents (including reporting a breach of confidentiality and disciplinary procedures for employees that breach confidentiality policies).

3. Storage of Claims: Paper claims should be stored in a file cabinet that is locked when not in use. No files containing PHI shall be left out on a desk overnight.

4. Access to Claims Office: Only the insurer's claims office personnel will be given keys or key codes to enter the office. Personnel should not enter an individual office or work area unless they have a business purpose for doing so.

5. Computer Access: A password shall be required to log onto a computer, and screens should be automatically turned off if activity does not occur for 15 minutes. Passwords must be at least eight characters long, a combination of numbers and letters, and must be changed every 90 days (some are changed monthly). Accounts will be locked out after three invalid attempts to log in. Insurer's claims office employees must not share their password information with anyone.

6. Fax: Fax machines should be in secure locations and be monitored regularly (e.g. every 30 minutes) for incoming documents. Fax machines should be turned off each night (if feasible). All outgoing faxes must have a cover sheet with a confidentiality statement.

7. Discussion Areas: Access to physical areas where participants and beneficiaries discuss benefit issues with the insurer's claims staff should be limited. Conversations about individual benefit issues by individuals who are not involved in payment or health care operations functions regarding that individual are prohibited. Care should be taken to avoid conversations in public areas.

8. Computer Network: Access controls (user-based, role-based or context based) should be implemented and included in the administrative operations and system network controls. The insurer and administrator will install firewalls to protect confidential information from internet exposure.

9. Termination of Employees: Upon final departure of any terminated employees, the insurer and the administrator will collect all keys and delete the passwords of such terminated employees.

10. Electronic Transmission: Any and all electronic transmissions of data will be encrypted using a dual key 128-bit encryption.

11. Disaster Recovery Program: The insurer and the administrator will create a disaster recovery program for loss of data due to fire, vandalism, natural disaster, or other system failure. Back up tapes are

created nightly by the insurer and the administrator and sent to an offsite data storage facility that stores these tapes in a data safe.

12 Shredding: After appropriate use is complete, documents containing PHI will be shredded before disposal, subject to the time frames specified in the Trust's record retention policy.

13. Hardware Disposal: Prior to disposal, hard drives of all computers shall be erased so that no claims data remains and none can be recovered by any known recovery method.

14. Audit Trails: The insurer and the administrator will monitor access to information stored on their systems through the use of audit trails.

15. Mail: Appropriate precautions must be taken when opening mail to assure that documents containing PHI are secure. Mail is opened in separate "mail rooms" and the buildings are secure.