TIMBER PRODUCTS MANUFACTURER'S TRUST
PRIVACY POLICY

INTRODUCTION

The Timber Products Manufacturers Trust ("Trust") is a group health plan and, thus, a Covered Entity as defined by the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A of the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), and the regulations promulgated thereunder, including the Final Omnibus Rule published on January 25, 2013 by the Department of Health and Human Services (collectively, "HIPAA"). The Trust and Business Associates who are retained by the Trust to perform or assist in the performance of one or more of the functions or activities of the Trust will create, receive, access, use, disclose or maintain Protected Health Information (PHI). The purpose of this policy is to provide guidelines for the Trust for compliance with the privacy and security standards of HIPAA and to protect the confidentiality of PHI.

POLICY

It is the policy of the Trust that PHI maintained by the Trust should be secured, maintained and released in accordance with applicable federal and state laws, rules and regulations, including HIPAA. All members of the Trust's Workforce who generate, use or otherwise deal with PHI should uphold the Trust Participant's confidentiality. This policy refers to all information resources, whether written, verbal, or electronic, and whether individually controlled, shared, stand alone or networked.

1. DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in HIPAA.

A. **Business Associate**. "Business Associate" has the meaning given such term in 45 C.F.R. §160.103. In general, a Business Associate is a person or entity, other than a member of the Trust's workforce, that performs certain functions or activities that involve the creation, receipt, use, maintenance or transmission of PHI on behalf of, or provides services to the Trust. A Subcontractor who creates, receives, maintains or transmits PHI on behalf of a Business Associate is also a Business Associate. Business Associate functions may include, but are not limited to: claims processing or administration, data analysis, consulting, accounting services, legal services, utilization review, quality assurance, benefit management, repricing and billing.

B. **Breach**. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI.

C. **Breach Notification Rules**. "Breach Notification Rules" shall mean the regulations set forth at 45 C.F.R. Part 164, Subpart D.

D. **De-Identified PHI.** "De-Identified PHI" is health information which does not identify an individual and cannot reasonably be believed to allow the identification of the individual.

E. **Designated Record Set**. "Designated Record Set" means the enrollment, payment, claims adjudication, and case or medical management records maintained by or for the Trust.

F. **Disclosure**. "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the Trust.

G. **Electronic Protected Health Information**. "Electronic Protected Health Information" or "EPHI" is PHI that is transmitted by electronic media, as that term is defined in 45 C.F.R. §160.103, or stored in electronic media.

H. **Genetic Information**. "Genetic Information" has the same meaning given such term in 45 C.F.R. §160.103 and, with respect to an individual, includes information about the individual's genetic tests, the genetic tests of family members of the individual, the manifestation of a disease or disorder in family members of such individual or any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

I. **Limited Data Set**. "Limited Data Set" shall have the same meaning given to such term in 45 C.F.R. §164.514(e)(2).

J. **Participant**. "Participant" means any individual who becomes eligible to participate in the benefits of the Trust's group health plan in accordance with the rules established for eligibility by the Trust.

K. **Privacy Rule**. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164.

L. **Protected Health Information**. "Protected Health Information" or "PHI" as defined in 45 C.F.R. § 160.103, includes information collected from an individual by the Trust which relates to past, present or future physical or mental health care or conditions of an individual or the provision of health care to an individual and which identifies the individual or could be reasonably believed to allow the identification of the individual. PHI for this policy refers to both PHI and electronic PHI (EPHI).

M. **Required By Law**. "Required By Law" shall have the same meaning given to such term in 45 C.F.R. § 164.103.

N. **Secretary**. "Secretary" shall mean the Secretary of the Department of Health and Human Services or their designee.

O. **Security Rule**. "Security Rule" shall mean the Security Rule at 45 C.F.R. Part 160 and Subparts A and C of 45 C.F.R. Part 164.

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

Q. **Underwriting Purposes**. "Underwriting Purposes" shall have the same meaning given to such term in 45 C.F.R. §164.502(a)(5)(i)(A) and, generally, shall mean: 1) Rules for, or determination of eligibility for, or determination of benefits under a health plan; 2) The computation of a premium or contribution amounts under the health plan; 3) The application of any pre-existing condition exclusion under the health plan; and 4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

R. **Unsecured PHI**. "Unsecured PHI" shall have the same meaning given to such term in 45 C.F.R. § 164.402.

S. **Use**. "Use" means, with respect to any PHI, the sharing, employment, application, utilization, examination, or analysis of such PHI within an entity that maintains such information.

T. **Workforce**. "Workforce" is defined to include employees, volunteers, trainees and other persons under the direct control of the Trust.

2. USE AND DISCLOSURE OF PHI

2.1 Permitted Use and Disclosure without Patient Authorization

2.1.1 Health Care Operations. The Trust may Use and Disclose PHI for health care operations. Healthcare Operations includes any of the following activities: quality assessment and improvement activities, competence and health plan performance reviews, training, accreditation, certification, licensing, credentialing and other related activities, case management activities, underwriting and other insurance related activities, providing alternative treatment and other health-related benefit information, medical review, legal services, auditing functions including fraud and abuse detection and compliance programs, business planning and development, business management and general administration activities. This list is not exhaustive and the Privacy Officer for the Trust should be contacted if there is a question as to whether an activity constitutes a health care operation.

2.1.2 Payment Operations. The Trust may Use and Disclose PHI for payment operations. In general, any processing activity which is necessary to process claims for reimbursement from the Trust to a healthcare provider who has provided treatment or services is regarded as a payment operation activity. The Privacy Officer for the Trust should be contacted if there is a question as to whether an activity constitutes a payment operation.

2.1.3 Other Permitted Uses and Disclosures. The Trust may use or disclose PHI without authorization in the following circumstances, subject to all applicable legal requirements and limitations:

- **For Public Health Activities:** The Trust may disclose PHI for the following public health activities and purposes:
  a. To report health information to public health authorities that are authorized by law to receive such information for the purpose of controlling disease, injury or disability.
  b. To report child abuse or neglect to a government authority that is authorized by law to receive such reports.
  c. To report information about a product or activity that is regulated by the U.S. Food and Drug Administration (FDA) to a person responsible for the quality, safety or effectiveness of the product or activity.
  d. To alert a person who may have been exposed to a communicable disease, if the Plans are authorized by law to give this Notice.
- **Health Oversight Activities:** The Trust may disclose PHI to a government agency that is legally responsible for oversight of the health care system or for ensuring compliance with the rules of government benefits programs, such as Medicare or Medicaid, or other regulatory programs that need health information to determine compliance.
- **To comply with the Law:** The Trust may use and disclose PHI to comply with the law or as Required By Law.
- **Judicial and Administrative Proceedings:** The Trust may disclose PHI in a judicial or administrative proceeding or in response to a legal order.
- **Law Enforcement Officials:** The Trust may disclose PHI to the police or other law enforcement officials, as required by law or in compliance with a court order or other process authorized by law.
- **For the health and safety of the General Public:** The Trust may disclose PHI to prevent or lessen a serious and imminent threat to your health and safety or the health and safety of the general public.
- **Various Government Functions:** The Trust may disclose PHI to various departments of the government such as the U.S. military or the Centers for Disease Control.

- **For Workers' Compensation:** The Trust may disclose PHI when necessary to comply with workers' compensation laws.
- **OTHER:** The Trust may disclose PHI when necessary to file claims with reinsurers or stop-loss carriers or to obtain coverage with reinsurers or stop-loss carriers. The Trust may also disclose PHI to subrogation vendors to recoup payments made by the Trust that were reimbursed by other insurance arrangements.

2.2 Uses and Disclosures requiring Authorization from the Participant

2.2.1 Written Authorization Requirement. PHI may be used for any purpose if the Participant has authorized in writing the use or disclosure in advance. Conversely, except for uses and disclosures set forth in Section 2.1, the Trust may not use or disclose protected health information without a valid authorization. An authorization is always required for the use and disclosure of PHI for marketing purposes, for the sale of PHI and for the use or disclosure of psychotherapy notes. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

2.2.2 Authorization Form. The authorization to be signed by the Participant must be obtained utilizing the current form approved by the Privacy Officer. The form must be signed by the Participant prior to using or disclosing the Participant's PHI. A copy of the signed authorization form should be provided to the Participant and the original shall be retained by the Privacy Officer.

2.2.3 Compound Authorizations. An authorization for use or disclosure of PHI for marketing purposes, the sale of PHI or the use or disclosure of psychotherapy notes may not be combined with any other document to create a compound authorization.

2.2.4 Conditional Authorizations. The Trust will not require a patient to sign any authorization as a condition of treatment, payment, enrollment or eligibility for benefits.

2.2.5 Revocation of Authorization. A Participant is allowed to revoke an authorization previously provided to the Trust by sending a written request to the Privacy Officer. The revocation shall be valid upon receipt of the form by the Privacy Officer except with respect to any authorized actions the Trust had already taken prior to receiving the revocation.

2.3 Business Associates

2.3.1 Use of Business Associates. Business Associates are allowed to create and receive PHI on behalf of Trust only after the Trust receives satisfactory assurance in the form of a written agreement that the Business Associate will safeguard and protect the PHI. The Privacy Officer is empowered to develop procedures and processes to evaluate a Business Associate's compliance with the requirements set forth in the Business Associate Agreement.

2.3.2 Business Associate Agreement. Any Business Associate Agreement used by the Trust shall contain the necessary provisions which ensure compliance with the Privacy Rule and the Security Rule. Any Business Associate Agreement presented to a Business Associate by the Trust shall be approved by the Privacy Officer. The Business Associate Agreement must be signed by the Trust and Business Associate prior to the commencement of any functions or activities by the Business Associate on behalf of the Trust.

2.4 Minimally Necessary Standard. Any use or disclosure of PHI is subject to the "minimum necessary" standard set forth 45 C.F.R. § 164.514(d). The "minimum necessary" standard requires the Trust and its Business Associates to restrict access and use of PHI to those individuals in their Workforce who need the PHI to carry out their duties and to limit the amount of PHI disclosed to an amount reasonably necessary to accomplish the underlying purpose of the disclosure.

2.5 De-Identified Information. The Trust may freely use and disclose De-Identified information.

3. SAFEGUARDING PHI

3.1. Access by Trust's Workforce. Members of the Trust's Workforce are not permitted to access or attempt to access PHI unless required as part of their employment duties and only if expressly informed of their right of access to PHI by an immediate superior. The Privacy Officer shall maintain a list of all employees authorized to have such access and the dates their authorized access began and ended. Appropriate safeguard procedures shall be implemented by the Privacy Officer to limit unauthorized access including use of door locks, locking file cabinets, computer screen protection, cardkeys, locked trash receptacles, passwords and/or other means of restricting physical access.

3.2. Access by others. Any Business Associates and Subcontractors, consultants, auditors, counsel, or others who will need access to PHI or may see PHI as part of their work for the Trust will be permitted access to PHI only as required to carry out their duties and only after signing a business associate agreement.

3.3. Storage of PHI

3.3.1. Storage in Work Stations and Work Areas. Files and records containing PHI should be stored in locked file cabinets or other repositories in areas inaccessible to persons other than those authorized to use the files and records. Documents containing PHI should not be left unattended in any work area or work station and should be handled in such a way as to minimize the possibility of any inadvertent viewing by persons not authorized to use the PHI. In addition, documents containing PHI should not be discarded in trash or recycling receptacles but shall be shredded or placed in bins designated for the disposal of documents containing PHI.

3.3.2. Electronic Storage of PHI. PHI and EPHI created or stored in electronic format (*e.g. such as on a computer hard drive, computer storage disks, copiers, corporate network drives and the like)* shall be protected by commercially appropriate methods. The data shall be backed up frequently in accordance with Trust's documented policies and procedures. All archived PHI shall be maintained at a site with appropriate security to prevent unauthorized access. All EPHI stored on any device (e.g. computer hard drives, copy machines, computer storage disks) shall be deleted from the device prior to disposing of the device and/or retiring the device. The Privacy Officer shall maintain an inventory of all devices which have the capability to create or store PHI.

3.3.3. Access to Electronically Stored PHI. All PHI access shall be restricted exclusively through the use of pre-assigned passwords assigned solely to authorized employees and based on the rights and access privileges granted to the employee based on their job description. Employees are expressly prohibited from disclosing their password to anyone. Any assigned passwords shall be permanently taken out of service upon the employee's termination of employment. Any Business Associate, Subcontractors, consultant, auditor, counsel, or others who will need access to electronically stored PHI or may see PHI and EPHI as part of their work for the Trust shall be given unique passwords which will be permanently taken out of service upon completion of their assigned work. Documentation shall be maintained regarding the assignment of the password and the subsequent expiration of the password will be maintained by the Privacy Officer.

3.3.4. Storage of PHI on Cloud Computing Services. For purposes of this policy, the phrase "Cloud Computing Services" shall mean any application or infrastructure which allows for web-based access to data storage and retrieval on a database which is not owned or maintained by

the Trust or one of its affiliates or business partners. Cloud Computing Services are not permitted for Trust business purposes unless the Trust has a signed license agreement with the vendor, even if the contract offered is a click through agreement (where you just click to accept online). All licensing agreements must be reviewed and approved by the Privacy Officer prior to any use of the service. No member of the Trust's Workforce is permitted to post PHI on any Cloud Computing Service unless the Trust has signed a valid license agreement or the Privacy officer has provided a written exception to this policy.

3.4. Electronic Transmission of PHI. All EPHI must reside on a secure network. Any transmission of EPHI must utilize an encryption mechanism to ensure the integrity and confidentiality of the PHI.

4. USE OF GENETIC INFORMATION

The Trust shall not use or disclose Genetic Information for Underwriting Purposes.

5. PARTICIPANT RIGHTS

5.1 Right to request additional restrictions. Participants may request restrictions on the use and disclosure of the Participant's PHI. Any request for additional restrictions needs to be submitted by the Participant in writing and shall include a)what information the Participant wants to limit; b) whether the Participant wants to limit the use, disclosure or both; and c) to whom the Participant wants the limits to apply. The Trust is not required to agree to a requested restriction but will attempt to honor such requests if, in the sole discretion of the Trust, the requests are reasonable. The Privacy Officer is charged with responsibility for administering requests for restrictions.

5.2 Right to receive confidential communications. Participants may ask to receive communications of their PHI from the Trust by alternative means of communication or at alternative locations. Although the Trust will consider reasonable requests carefully, the Trust is not required to agree to all requests. The Trust shall accommodate such a request if the Participant clearly states that the disclosure of all or part of that information by a means other than requested could endanger the Participant. The Privacy Officer has responsibility for administering requests for confidential communications.

5.3 Right to inspect and copy PHI. Participants may ask to inspect or to obtain a copy of their PHI that the Trust maintains in a Designated Record Set and request the form and format, including an electronic form and format, they wish to use to access their PHI. The Trust will honor a request to provide access in the form and format requested so long as it is readily producible in such form and format; or if not, in a readable electronic form and format as agreed to by the Trust and the Participant. Under limited circumstances, the Plans may deny you access to a portion of your records. The Trust must provide a response to the Participant within 30 days after receipt of the request.

5.4 Right to amend records. A Participant has the right to ask the Trust to amend PHI that is contained in the Trusts records if the Trust determines that the record is inaccurate, and the law permits the Trust to amend it. Requests for an amendment need to be submitted in writing. The Trust may deny a request for an amendment if it is not in writing or does not include a reason to support the request. In addition, the Trust will deny a request to amend information that:

- Was not created by the Trust, unless the person or entity that created the information is no longer available to make the amendment.
- Is not part of the medical information that is or would be kept by the Trust.
- Is not part of the information that the Participant would be permitted to inspect and copy.
- Is accurate and complete.

The Trust shall provide a response to the Participant's request within 60 days of receiving the request.

5.5 Right to receive an accounting of disclosures. A Participant has the right to obtain an accounting of any unauthorized disclosures of PHI which do not satisfy the exceptions set forth in Section 2.1 made in

the last 6 years and of any disclosures of Genetic Information made in the last 6 years. The Trust shall respond to an accounting request within 60 days. If the Trust is unable to provide the accounting within 60 days, it may extend the period by 30 days provided that it gives the Participant notice within the original 60 day period of the reason for the delay and the date the information will be provided. The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

6. BREACHES OF PHI

HIPAA imposes stringent requirements upon the Trust to safeguard the privacy of a Participant's PHI. The Trust may be subject to sanctions and enforcement actions for a Breach of Unsecured PHI and for failing to properly report a Breach of Unsecured PHI.

6.1 Duty to Inform Privacy Officer of Alleged or Suspected Breaches. Any confirmed or suspected Breach of PHI, or allegations received from any individual or entity that there has been a Breach shall be reported to the Privacy Officer. The Privacy Officer shall maintain a record of any confirmed, suspected or alleged Breach notifications which are received.

6.2 Duty to Investigate Suspected Breaches. The Privacy Officer is responsible for investigating any confirmed, suspected or alleged Breach of PHI. Such investigation may include conducting reviews, contacting employees, Workforce members or Business Associates, and working with other Trust resources as needed. The initial investigation shall include a determination of whether the use and disclosure is a permitted use or disclosure and, if not, whether any of the exclusions from the definition of Breach set forth in 45 C.F.R. §164.401 apply.

6.3 Presumption of Breach. For purposes of determining the existence of a Breach, there is a presumption that any acquisition, access, use, or disclosure of PHI in violation of HIPAA is a reportable Breach.

6.3 Risk Assessment Factors. The following risk assessment factors shall be evaluated and documented by the Privacy Officer in order to determine the existence of a reportable breach when a presumption of a breach exists: 1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; 2) The unauthorized person who used the PHI or to whom the disclosure was made; 3) Whether the PHI was actually acquired or viewed; and 4) The extent to which the risk to the PHI has been mitigated.

6.4 Duty to Report Breaches. The Privacy Officer has responsibility to notify a Participant of a Breach and complying with all Breach Notification Rules.

6.5 Business Associates. Business Associates shall, following the discovery of a Breach of Unsecured PHI, notify the Trust of such Breach. A Business Associate's obligation to notify the Trust of any Breach shall be set forth in any Business Associate Agreement between the Trust and a Business Associate.

7. NOTICE OF PRIVACY PRACTICES

The Privacy Officer is responsible for developing and maintaining a Notice of Privacy Practices which describes how medical information about the Participant may be used and disclosed by the Trust and how the Participant can get access to this information. A current Notice of Privacy Practices shall be provided to all Participants.

8. TRAINING

As a condition of employment all members of the Workforce are required to participate in training. Additionally, the Trust may require any member of the Workforce to take and pass a test regarding HIPAA. The record of the test and an indication that the employee passed the test are part of the Workforce member's personnel file.

9. PRIVACY OFFICER

Trust has appointed a Privacy Officer who will have primary responsibility for ensuring system-wide compliance with HlPAA security and privacy regulations. The current Privacy Officer and the contact information for the Privacy Officer is set forth in the current Notice of Privacy Practices. The responsibilities of the Privacy Officer include, but are not limited to: (i) development and implementation of the policies and procedures relating to privacy; (ii) oversight of issues in conformance with privacy legislation; (iii) establishment of a process for receiving, documenting, tracking, investigating, taking action on complaints concerning privacy policies and procedures, and maintaining records of all complaints and their disposition; (iv) oversight of training for the Workforce, volunteers, contractors, business associates and other appropriate third parties; (v) promotion of activities to foster information privacy awareness; (vi) assistance with the development of Business Associate and Notice of Privacy Practices agreements, as well as other pertinent policies and procedures; and (vii) undertake periodic risk assessments to ensure that any potential risks and vulnerabilities inherent in any existing or newly acquired technology are known and adequately addressed by the Trust.

10. VIOLATION OF PRIVACY POLICY

Wrongful disclosure and/or use of PHI may result in immediate disciplinary action up to and including termination of employment.

11. COMPLAINT PROCESS

The Notice of Privacy Practices provides Participants with the contact information for the Privacy Officer. Complaints of alleged privacy violations can be received through multiple channels: in person, in writing or by telephone. Any member of the Trust's Workforce who is involved in events which are or appear to be violations of this policy, or who gains direct knowledge that a subordinate, co-worker, or supervisor is involved in events which are or appear to be in violation of this policy, must immediately report such events to Human Resources or the Privacy Officer. The Trust will not retaliate nor tolerate retaliation by others against any person who, in good faith, reports activities of another which are, or appear to be, violations of this policy.