HIPAA Notice of Privacy Practices

THIS NOTICE OF PRIVACY PRACTICES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GAIN ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices (the "Notice") describes the legal obligations of [Employer] group health Plan (the "Plan") and your legal rights regarding your protected health information held by the Plan under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Among other things, this Notice describes how your protected health information may be used or disclosed to carry out treatment, payment, or healthcare operations, or for any other purposes that are permitted or required by law.

We are required to provide this Notice of Privacy Practices to you pursuant to HIPAA.

The HIPAA Privacy Rule protects only certain medical information known as "protected health information." Generally, protected health information is individually identifiable health information, including demographic information, collected from you or created or received by a healthcare provider, a healthcare clearinghouse, a health Plan, or your employer on behalf of a group health Plan, that relates to the following:
(1) your past, present or future physical or mental health or condition;
(2) the provision of healthcare to you; or
(3) the past, present or future payment for the provision of healthcare to you.
If you have any questions about this Notice or about our privacy practices, please contact Terry McLoughlin, CFO (HIPAA Officer) or Tim Hulett, Human Resources Manager.

Effective Date

This Notice is effective 06/01/2013

HIPAA Privacy Policy

Shearer Automotive sponsors Health Plans subject to the HIPAA Privacy Rules. Certain employees may have access to the individually-identifiable health information of Plan Participants as it relates to the administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Company's ability to use and disclose protected health information:

> Protected health information means information that is created or received by the Plan and
>
> (a) relates to the past, present, or future physical or mental health or condition of a Participant;
>
> (b) relates to the provision of healthcare to a Participant;
>
> (c) relates to the past, present, or future payment for the provision of healthcare to a Participant; or
>
> (d) identifies the Participant and suggests a reasonable likelihood that the information might be used to identify the Participant. Protected health information includes information of persons living or deceased.

The Plan intends to fully comply with HIPAA's requirements. Those with access to PHI must comply with this policy. The Plan reserves the right to amend or change this policy at any time without notice. To the extent that this policy establishes requirements and obligations above and beyond those required by HIPAA, the policy shall not be binding upon the Company. This policy does not address requirements under other federal or state laws.

Shearer Automotive HIPAA Privacy Rules

1. Plan Identities:

Blue Cross Blue Shield Medical Insurance HDHP Plan
Delta Dental Insurance
UNUM Basic and Optional Life Insurance and AD&D
UNUM Short Term Disability Insurance

2. Health information received or created by the Plan: (Check all that apply.)
X Enrollment and dis-enrollment by employee
X Plan Administrative Functions

> **Known uses for the health information**:
> Plan enrollment, Claims, Plan Administration, and Renewal
> Medical leaves of absence / FMLA

3. List internal personnel with access to the above health information:
a. Terry McLoughlin, CFO
b. Judy Cheney, Office Manager
c. MaryJo DuBois, Office Manager
d. Karen Barcomb, Office Manager
e. Laurel Chapman, Office Manager
f. Kevin Bowie, General Manager
g. Tim Hulett, Human Resources Manager

The above-named employees are involved in the administration of the employer's Plan. They understand that their access will be limited to the minimum information necessary for them to perform their duties associated with the Plan. These individuals are required to review and understand the employer's Privacy Policy as well as the procedures the employer has adopted to comply with the HIPAA Privacy Requirements.

4. Training of staff members with access to PHI

The following staff members have been trained on this policy and understand their responsibilities in handling PHI, as attested by signature and date below:
a. Name _Terry McLoughlin, CFO_____ Date training completed _08/07/2013___
b. Name _Judy Cheney, Controller_____ Date training completed _08/07/2013___
c. Name _MaryJo DuBois, Office Manager Date training completed _08/07/2013___
d. Name _Karen Barcomb, Office Manager Date training completed _08/07/2013___
e. Name _Laurel Chapman, Office Manager Date training completed _08/26/2013___
f. Name _ Kevin Bowie, General Manager Date training completed _08/26/2013___
g. Name _Tim Hulett, HR Manager_____ Date training completed _08/07/2013___

Plan Responsibilities

1. Privacy Officer and Contact Person
Terry McLoughlin, CFO is the Privacy Officer for the Plan, and as such, is responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Policy and the Company's HIPAA policies and procedures. The Privacy Officer will also serve as contact person for Participants who have questions, concerns, or complaints about the privacy of their PHI.

2. Education and Training
This Company will inform and educate all employees with access to PHI about its various privacy policies and procedures.

3. **Safeguards and Firewall**
The Company will establish, on behalf of the Plan appropriate safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's Privacy rules. Safeguards include limiting access to information by creating computer firewalls. Other safeguards include locking doors on filing cabinets. Firewalls will ensure that only authorized employees may access PHI, that they may access only the minimum amount of PHI necessary for Plan administrative functions, and that they may not further use or disclose PHI.

4. **Privacy Notice**
The Privacy Officer is responsible for developing and maintaining a notice of the Plan's privacy practices that describes the use and disclosure of PHI, the individual's rights, and the Plan's legal duties with respect to PHI. This notice will inform Participants that the Company will have access to PHI in connection with Plan administrative functions. The privacy notice will also provide a description of the Company's complaint procedures, along with the name of the contact person to whom complaints may be voiced.

The Notice of Privacy Practice must be provided to any new employee at the time of Plan enrollment and within 60 days after a material change has been made to the notice. The employer should also provide notice of availability of the privacy notice at least every three years.

5. **Complaints**
The Privacy Officer will be the Plan's contact person for receiving complaints and concerns. This person will be responsible for creating a process for individuals to lodge complaints and for creating a system for handling such complaints.

6. **Violations**
Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with the employer's discipline policy, up to and including termination of employment.

7. **Mitigation of Inadvertent Disclosure of PHI**
To the extent possible the employer shall mitigate any harmful effects from use or disclosure of an individual's PHI in violation of the set policies and procedures. As a result, if an employee becomes aware of a disclosure of protected health information, the Participant should immediately contact the Privacy Officer so that steps can be taken to expeditiously mitigate any harm to the Participant.

8. **No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy**
No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility.

9. **Plan Document**
The Plan Document shall include provisions for describing both permitted and required Company uses and disclosures of PHI for Plan administrative purposes. Specifically the Plan Document shall require that the employer does the following:
• Not use or further disclose PHI other than as permitted by the document or required by law.
• Ensure that any agents or subcontractors to whom it provides PHI agree to the same restrictions and conditions that apply to the Company.
• Not use or disclose PHI for employment-related actions or in connection with any other employee benefit Plan.
• Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.
• Make PHI available to Plan Participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures.
• Upon request, make available to Department of Health and Human Services the Company's internal practices and records relating to the use and disclosure of PHI received from the Plan.
• If feasible, return or destroy all PHI received from the Plan and retain no copies of such information when no longer needed for their original purpose, unless such return or destruction is not feasible, or would limit subsequent uses and disclosures.

The Plan Document must also require the Company to certify to the Privacy Officer that the Plan Documents have been amended to include the above restrictions and that the Company agrees to those restrictions and provides adequate firewalls.

10. **Documentation**
The Plan's and the Company's Privacy Policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the Privacy Policy must be revised promptly and made available. Such a change is effective only with respect to PHI created or received after the effective date of the notice.

The Plan and the Company shall document certain events and actions relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years.

Use and Disclosure of PHI

1. **Use and Disclosure Defined**
The Company and the Plan will use and disclose PHI only as permitted under HIPAA. The terms are defined as follows:

Use: The sharing, employment, application, utilization, examination, and/or analysis of individually-identifiable health information by any person working for or within the benefits department of the Company, or by a Business Associate of the Plan.

Disclosure: For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually-identifiable health information to a person or persons not employed by or working within the Company's benefits department.

2. **Workforce Must Comply with Company's Policy and Procedures**
All members of the Company's workforce with access to PHI (described at the beginning of the Policy and referred to herein as "employees") must comply with this Policy and with the Company's more detailed use and disclosure procedures, which are set forth in a separate document.

3. **Permitted Uses and Disclosures – Payment and Healthcare Operations**
PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another entity for the covered entity's payment purposes.

Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for providing benefits under the Plan or activities to obtain or provide reimbursement for healthcare. Payment also includes the following:

• Eligibility and coverage determinations, including coordination of benefits and adjudication of health benefit claims.
• Risk adjusting based on enrollee status and/or demographic characteristics.
• Billing, claims management, collection activities and/or obtaining payment under a contract for reinsurance and related healthcare data processing. PHI may be disclosed for purposes of the Plan's own healthcare operations. PHI may be disclosed to another covered entity for quality

assessment and improvement, for case management, or for healthcare fraud and abuse detection programs, if the covered entity has a relationship with the Participant and the PHI requested pertains to that relationship. Healthcare operations means any of the following activities to the extent that they relate to Plan administration:
• Conducting quality assessment and improvement activities.
• Reviewing healthcare performance.
• Underwriting and premium rating.
• Conducting or arranging for medical review, legal services, and auditing functions.
• Business planning and development.
• Business management and general administrative activities.

4. **PHI Disclosures that are Permitted**
While PHI may be disclosed in various situations without a Participant's authorization, the employer's policy and procedure on use and disclosure should describe any specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Company's Privacy Officer. Disclosures are permitted under the following circumstances:

• In instances regarding victims of abuse, neglect or domestic violence.
• Judicial and administrative proceedings.
• Law enforcement purposes.
• Public health activities.
• Health oversight activities.
• Decedent's request.
• Cadaveric organ, eye, or tissue donation purposes.
• Certain limited research purposes.
• Serious threats to health and/or safety.
• Specialized government functions.
• Workers' compensation programs.

PHI may be disclosed for any purpose if the Participant provides an authorization that satisfies all of HIPAA's requirements. All uses and disclosures made pursuant to a signed authorization must be consistent with the organization's terms and conditions.

5. **"Minimum" Necessary Requirements**
When PHI is used or disclosed, HIPAA requires that the information disclosed must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. The minimum necessary standard does not apply to any of the following:
• Uses or disclosures made to the individual.
• Uses or disclosures made pursuant to a valid authorization.
• Disclosures made to the DOL.
• Uses or disclosures required by law.
• Uses or disclosures required to comply with HIPAA.

Employees may disclose PHI to the Plan's Business Associates and allow the Plan's Business Associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first

obtain assurances from the Business Associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a Business Associate, employees must contact the Privacy Officer and verify that a Business Associate Agreement is in place.

Individual Rights

Employees have the following rights with respect to their protected health information:

Right to Inspect and Copy. You have the right to inspect and copy certain protected health information that may be used to make decisions about your healthcare benefits. To inspect and copy your protected health information, you must submit your request in writing to the Privacy Officer. If you request a copy of the information, we may charge a reasonable fee for the costs of copying, mailing, or other supplies associated with your request.

The company may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to your medical information, you may request that the denial be reviewed by submitting a written request to the Privacy Officer.

Right to Amend. If you think the protected health information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Plan.

To request an amendment, your request must be made in writing and submitted to the Privacy Officer. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, if you ask us to amend information, we may deny your request for the following reasons:

• it is not part of the medical information kept by or for the Plan;
• it was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
• it is not part of the information that you would be permitted to inspect and copy; or
• it is already accurate and complete.
If we deny your request, you have the right to file a Statement of Disagreement with us and any future disclosures of the disputed information will include your statement.

Right to an Accounting of Disclosures. You have the right to request an "accounting" of certain disclosures of your protected health information. The accounting will not include (1) disclosures for purposes of treatment, payment, or healthcare operations; (2) disclosures made to you; (3) disclosures made pursuant to your authorization; (4) disclosures made to friends or family in your presence or because of an emergency; (5) disclosures for national security purposes; and (6) disclosures incidental to otherwise permissible disclosures.

To request this list or accounting of disclosures, you must submit your request in writing to the Privacy Officer. Your request must state a time period of no longer than six years and may not include dates before April 14, 2003. Your request should indicate in what form you want the list (for example, paper or electronic). The first list you request within a 12-month period will be provided free of charge. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to Request Restrictions. You have the right to request a restriction or limitation on your protected health information that we use or disclose for treatment, payment, or healthcare operations. You also have the right to request a limit on your protected health information that we disclose to someone who is involved in your care or the payment for your care, such as a family member or friend. For example, you could ask that we not use or disclose information about a surgery that you had.

Except as provided in the next paragraph, we are not required to agree to your request. However, if we do agree to the request, we will honor the restriction until you revoke it or we notify you.

Effective February 17, 2010 (or such other date specified as the effective date under applicable law), we will comply with any restriction request if: (1) except as otherwise required by law, the disclosure is to the health Plan for purposes of carrying out payment or healthcare operations (and is not for purposes of carrying out treatment); and (2) the protected health information pertains solely to a healthcare item or service for which the healthcare provider involved has been paid out-of-pocket in full.

To request restrictions, you must make your request in writing to the Privacy Officer. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure, or both; and (3) to whom you want the limits to apply—for example, disclosures to your spouse.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we contact you at work or by mail only. To request confidential communications, you must make your request in writing to the Privacy Officer. We will not ask you the reason for your request. Your request must specify how or where you wish to be contacted. We will accommodate all reasonable requests if you clearly provide information that the disclosure of all or part of your protected information could endanger you.

Right to be Notified of a Breach. You have the right to be notified in the event that we (or a Business Associate) discover a breach of unsecured protected health information.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. You may obtain a copy of this notice at our website, http://1.sheareraauto.com/shearer.html. To obtain a paper copy of this notice, contact the Privacy Officer.

Complaints
If you believe that your privacy rights have been violated, you may file a complaint with the Plan or with the Office for Civil Rights of the United States Department of Health and Human Services. To file a complaint with the Plan, contact the Human Resources Department. All complaints must be submitted in writing. You will not be penalized, or in any other way retaliated against, for filing a complaint with the Office for Civil Rights or with us.

Procedures for Complying with Individual Rights

1. Request for Access
A Designated Record set is a group of records maintained by or for the employer, and includes the enrollment, payment and claims adjudication record of an individual maintained by the Plan. It also includes other protected health information used, in whole or in part, by or for the Plan when making coverage decisions about an individual.

Procedure
For disclosure of an individual's PHI, the employee must take the following steps:
• Verify the individual's identity.
• Determine whether the PHI is held in the designated record set.
• Determine whether an exception to the disclosure requirement might exist. See the Privacy Official as to whether any exception exists.
• Provide or deny the request within 30 days. If the PHI cannot comply with such a deadline, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 day period.
• A denial notice must contain the basis for the denial, a statement of the individual's right to request a review, and directions to the individual for filing a complaint concerning the denial.
• Provide the information in a readable format. Or provide in a format agreed to by the employee.
• At the discretion of the employer, additional fees may be charged for copying, postage and preparation.
• Disclosures must be documented in accordance with the Documentation Requirements procedure.

2. Request for Amendment Procedure
Upon Receipt of a request from an individual, from a parent of a minor child, or from a personal representative for an amendment to an employee's PHI in a designated record set, the employee must take the following steps:
• Verify the individual's identity.
• Determine whether the PHI at issue is held in the employee's designated record set. See the Privacy Official if the information does not seem to be held in designated record set.
• Determine whether the amendment is allowable under HIPAA's right to access.
• Determine whether the request for the amendment is appropriate.
• Respond to the request within 60 days by informing the individual whether the request has been accepted or denied. If a decision cannot be made within 60 days, the deadline may be extended for 30 more days.
• Upon acceptance of the amendment, make the change in the designated record set.

• Denied requests must do the following:
• The PO must review the denial. The denial must include the reason for the denial, information about the individual's right to disagree, an explanation that the individual may ask that the request for amendment and its denial be included in future disclosures of the information, and directions for filing a complaint concerning the denial.
• Under circumstances where the individual provides a Statement of Disagreement, include all specifics relating to the denial.

3. Processing Request for an Accounting of PHI Procedure
Upon the receipt of a request for an account of disclosures the following procedures must be followed:
• Verify the identity of the individual procedure.
• Inform the individual that there may be a fee charged if the employees have requested this information more than once in the last twelve months.
• Respond to the request within 60 days by providing the accounting, or by informing the individual that there have been no disclosures that must be included in an accounting. The 60 day deadline may be extended for an additional 30 days by written notice.
• The accounting must include any disclosures made by the Plan or by a Business Associate for up to six years prior to the request. Disclosures not included are:
• To carry out treatment, payment and healthcare operations.
• To the individual about his/her own PHI.
• Incidental to an otherwise permitted use or disclosure.

Pursuant to an individual authorization.
• For specific national security or intelligence purposes.
• To correctional institution or law enforcement when the disclosure was permitted without an authorization.
• As part of a limited data set.
• The accounting must include the date of disclosure, the name of the entity or person to whom the information was disclosed, a brief description of the PHI disclosed, and a brief statement explaining the purpose for the disclosure.
• If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would likely impede the agency's activities, then disclosure may not be required. The employee must contact the Privacy Official under these circumstances for more guidance.
• Accountings must be documented in accordance with the appropriate procedure.

4. Processing Request for Confidential Communications Procedure
In order for an individual to receive communications in an alternate format or location, the following steps must be followed:
• Verify the individual's identity as set forth in the appropriate procedures.
• Determine whether the request could endanger the individual.
• The employee should take steps to honor the request.
• If the request cannot be accommodated, the employees must contact the individual explaining why.
• All confidential requests will be maintained by the Privacy Officer.

• Requests and their dispositions must be documented in accordance with the appropriate procedure.

5. Processing Requests for Restriction on Use and Disclosures of PHI Procedure

Upon the permission for access employees must adhere to the following steps regarding an individual's PHI:

• Verify the individual's identity in accordance with the appropriate procedure.
• Take steps to honor the request.
• If the request cannot be accommodated, the employee must contact the individual explaining why.
• Track all requests on use or disclosures.
• Notify all Business Associates that may have access to the individual's PHI of any agreed-upon restrictions.
• Document requests and their dispositions in accordance with the appropriate procedure.

Unknown or Inadvertent Disclosure of PHI

A covered entity must mitigate, to the extent possible, any harmful effects that become known of disclosing an individual PHI in violation of the policies and procedures set forth in this policy. The Privacy Official must be contacted immediately of any incorrect use or disclosure of PHI.

Mitigation

If an inadvertent disclosure of PHI is made by a Shearer Automotive staff member the individual who's PHI was inadvertently disclosed to someone outside the bounds of this policy will be informed immediately, the disclosure will be recorded, dated, described, and tracked, and the staff member who inadvertently disclosed the PHI will be re-trained and counseled. The re-training and counseling will also be recorded.

Description of PHI incorrectly disclosed:	Affected Employee:	Disclosed by:	Date:	Signature of staff member retrained and counseled: