

ATTACHMENT C

**HIPAA PRIVACY AND SECURITY POLICY
for
Reliance Steel & Aluminum Co.**

Amended and restated as of January 1, 2017

TABLE OF CONTENTS

1. POLICY OVERVIEW AND HANDLING PROTECTED HEALTH INFORMATION.....	1
1.1 Overview of Policies and Procedures to Protect the Privacy and Security of Protected Health Information	1
1.2 Minimum Necessary Policy	3
1.3 Appointment and Duties of the Privacy Officer	4
1.4 Business Associate Agreements.....	5
1.5 Uses and Disclosures of Protected Health Information Authorization is Required/Not Required ...	6
1.6 Disclosures of Protected Health Information to the Company	8
1.7 Disclosures to Personal Representatives, Individuals, Family Members and Friends.....	10
1.8 Disclosures for Judicial and Administrative Proceedings.....	13
1.9 Uses and Disclosures Required by Law.....	15
1.10 Verification	16
1.11 Notice of Privacy Practices	17
1.12 De-Identified Information	18
1.13 [Reserved]	19
2. POLICIES REGARDING THE RIGHTS OF INDIVIDUALS UNDER THE HIPAA PRIVACY RULE.....	20
2.1 Access to Protected Health Information	20
2.2 Amendments to Protected Health Information	22
2.3 Complaints	24
2.4 Confidential Communications of Protected Health Information	25
2.5 Documenting Disclosures and Accountings	26
2.6 Requesting Restrictions on Uses and Disclosures of Protected Health Information	28
2.7 Genetic Information Nondiscrimination Act	29
3. POLICIES REGARDING ELECTRONIC PROTECTED HEALTH INFORMATION.....	30
3.1 In General.....	30
3.2 Administrative Safeguards.....	30
3.2.1 Security Risk Assessment, Security Management and Evaluation	30
3.2.2 Appointment and Duties of the Security Officer	31
3.2.3 Security Awareness and Training	31
3.2.4 Security Incident Procedures	32
3.2.5 Data Back-Up Plan.....	33
3.2.6 Disaster Recovery and Emergency Mode Plan	33
3.3 Physical and Technical Safeguards.....	33
3.3.1 Device and Media Controls.....	33
3.3.2 Access and Audit Controls.....	34
4. GENERAL POLICIES	35
4.1 Interpretation and Application of the Privacy Policy.....	35
4.2 Amending the Privacy Policy	36
4.3 Mitigation of Known Violations of the Privacy Policy	37
4.4 Record Retention and Documentation Policy	37
4.5 Refraining from Intimidating or Retaliatory Acts.....	39
4.6 Sanctions.....	40
4.7 Training Policy.....	41

5.	GLOSSARY	42
6.	APPENDIX	45
6.1	Plans Covered by the Privacy Policy	45
6.2	Privacy Officer, Security Officer and HIPAA Privacy Group Designations	46
6.3	Specific Rules for Access and Use of Protected Health Information	47
7.	FORMS AND NOTICES.....	49
7.1	FAQ's to Employees Regarding Data Privacy and Security Safeguards.....	49
7.2	Authorization for Use or Disclosure of Protected Health Information (General).....	53
7.3	Authorization for Use or Disclosure of Protected Health Information (Participant Assistance)	55
7.4	Authorization for Use or Disclosure of Protected Health Information (Participant Assistance – Spousal Appointment)	56
7.5	Business Associate Agreement	57
7.6	HIPAA Privacy Confidentiality Agreement	66
7.7	Protected Health Information Disclosure Log	67
7.8	Breach Notification Form Letter.....	68
7.9	Notice of Privacy Practices for Protected Health Information.....	71
7.10	Request for Access to Protected Health Information.....	77
7.11	Request to Amend Protected Health Information	78
7.12	Complaint Form	79
7.13	Request for Confidential Communications of Protected Health Information.....	80
7.14	Request for an Accounting of Disclosures of Protected Health Information.....	81
7.15	Request for a Restriction on Protected Health Information	83
7.16	Response to Individual's Request to Access Protected Health Information.....	84
7.17	Response to Individual's Request to Amend Protected Health Information	86
7.18	Data Breach Response Checklist	88
7.19	Assessment and Implementation Materials – Self Audit Form.....	91
7.20	Assessment and Implementation Materials – Administrative, Physical and Technical Checklists	94
7.21	Training Acknowledgement Form	98

1. POLICY OVERVIEW AND HANDLING PROTECTED HEALTH INFORMATION

1.1 OVERVIEW OF POLICIES AND PROCEDURES TO PROTECT THE PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

POLICY

The policies and procedures set forth in this manual (referred to collectively as the “Privacy Policy”) are intended to protect the privacy and security of Protected Health Information (“PHI”) in accordance with the privacy and security rules set forth in the Department of Health and Human Services (“HHS”) regulations at 45 CFR Part 160 and Part 164, Subparts A, D and E (“HIPAA Privacy Rule”) and 45 CFR Part 160 and Part 164, Subpart C (“HIPAA Security Rule”), as amended, including the Final HIPAA Rule issued by HHS on January 25, 2013.

The Privacy Policy shall apply to any and all Protected Health Information maintained, used or disclosed by or with respect to certain group health plans maintained by Reliance Steel & Aluminum Co. (collectively referred to as the “Plan”) as set forth in the Appendix to the Privacy Policy.

Except as otherwise provided for in the Privacy Policy, in the respective plan documents, or as permitted under the HIPAA Privacy Rule, only employees who are designated as members of the Company’s HIPAA Privacy Group shall have access to Protected Health Information maintained by the Plan. The members of the HIPAA Privacy Group shall be

- the Privacy Officer appointed pursuant to the Appointment and Duties of the Privacy Officer section of the Privacy Policy;
- the Security Officer appointed pursuant to the Appointment and Duties of the Security Officer section of the Privacy Policy; and
- the positions listed in the Appendix to the Privacy Policy.

For purposes of the Privacy Policy, members of the HIPAA Privacy Group shall, unless otherwise noted, be treated as acting on behalf of the Plan. An individual who is removed from the HIPAA Privacy Group for any reason, including disability, change of work assignment, vacation, or termination of employment for any reason, shall immediately return to the Company his or her security clearance, passwords, and all other equipment, devices or information that enables him or her to access, download, modify, or destroy Protected Health Information, except if authorized by the Privacy Officer.

The HIPAA Privacy Group shall maintain, use or disclose Protected Health Information in accordance with the procedures set forth in the Privacy Policy, including the procedures set forth in the Appendix, provided doing so does not result in a violation of the HIPAA Privacy Rule or the HIPAA Security Rule. No member of the HIPAA Privacy Group shall use or disclose Protected Health Information for employment related actions or decisions nor shall such member use or disclose such information in connection with any other benefit or employee benefit plan of the Company. Except as permitted under the HIPAA Privacy Rule, neither the Plan nor any of its business associates may receive remuneration in exchange for any Protected Health Information except as expressly authorized by the Individual in a valid authorization.

It is the intent of the Plan and the Company to comply with all relevant State laws governing health information privacy, unless preempted by the Employee Retirement Income Security Act (“ERISA”), the

HIPAA Privacy Rule or the HIPAA Security Rule. If any provision of the Privacy Policy is inconsistent with the HIPAA Privacy Rule, the HIPAA Security Rule or a more restrictive State privacy law, the Privacy Policy will be interpreted so that it complies with such law. Questions as to whether a State law applies to the Plan or is preempted by ERISA, the HIPAA Privacy Rule or the HIPAA Security Rule shall be resolved by the Privacy Officer or the Security Officer, as applicable.

Key terms are defined in the Glossary.

1.2 MINIMUM NECESSARY POLICY

POLICY

The HIPAA Privacy Group shall ensure that the PHI used and disclosed under the Privacy Policy is, to the extent required under the HIPAA Privacy Rule, only the minimum necessary to accomplish the purpose of the use or disclosure. This is done by identifying which workforce members need access to PHI to carry out their job functions; making reasonable efforts to limit the exposure of PHI to the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure, or request by establishing protocols that define the minimum necessary to perform routine uses, disclosures and requests and how to apply the minimum necessary to non-routine uses, disclosures and requests; and investigate any minimum necessary violations. Only the amount of PHI reasonably necessary to achieve the purpose of any particular use or disclosure should be disclosed.

PROCEDURE

1. Any requests for the use and/or disclosure of PHI shall be forwarded to and handled by members of the HIPAA Privacy Group. Unless otherwise provided in the Privacy Policy, only members of the HIPAA Privacy Group shall have access to PHI used, disclosed or maintained by the Plan.
2. In the event of a request for use or disclosure of an individual's entire medical record, such record may not be used or disclosed except when specifically justified as the amount that is reasonably necessary to accomplish the purpose of the request.
3. In the case of routine uses and disclosures of PHI, and unless as required under the Privacy Policy, a member of the HIPAA Privacy Group may make the use or disclosure which he or she reasonably believes is the minimum necessary to accomplish the purpose of the use or disclosure. Any non-routine use or disclosure of PHI shall be reviewed by the Privacy Officer prior to the use or disclosure.
4. Regardless of the requirements in the preceding paragraph, a member of the HIPAA Privacy Group may, if it is reasonable to do so, rely on a requested disclosure as the minimum necessary for the stated purpose if
 - the disclosure is to a public official who represents that the information requested is the minimum necessary for the stated purpose(s);
 - the information is requested by another Covered Entity; or
 - subject to Section 1.4, the information is requested by a Business Associate of the Plan for the purpose of providing certain services to the Plan, if the individual making the requests represents that the information requested is the minimum necessary for the stated purpose(s).
5. This minimum necessary policy shall not apply to:
 - Disclosures to or requests by a health care provider for treatment.
 - Uses or disclosures made to the individual who is the subject of the PHI.
 - Uses or disclosures made pursuant to an authorization.
 - Disclosures required for compliance to the Secretary of Health and Human Services.
 - Uses or disclosures that are required by law.
 - Uses or disclosures that are required for compliance with applicable requirements of the HIPAA Privacy Rule.

1.3 APPOINTMENT AND DUTIES OF THE PRIVACY OFFICER

POLICY

The Company, on behalf of the Plan, shall appoint a Privacy Officer (and set forth such appointment in the Appendix to the Privacy Policy) to implement and oversee compliance with the requirements of the HIPAA Privacy Rule.

The Privacy Officer is responsible for developing and implementing policies and procedures to comply with the HIPAA Privacy Rule as applicable to the Company and the Plan, developing employee training programs, publishing and distributing the Plan's notice of privacy practices and, except as otherwise provided in the Privacy Policy, serving as the designated decision maker for issues and questions involving interpretation of the HIPAA Privacy Rule, in coordination with the Security Officer and legal counsel. The Privacy Officer is responsible for the following tasks, as appropriate:

- Inventorying the uses and disclosures of all PHI as required under the HIPAA Privacy Rule.
- Working with legal counsel and management, key departments and committees to ensure the Company has and maintains appropriate consent and authorization forms and information notices, including amendments to plan documents, and negotiating Business Associate Agreements.
- Establishing and implementing appropriate firewalls between the Company and the Plan.
- Establishing structures to ensure individual rights guaranteed by the HIPAA Privacy Rule.
- Setting up a complaint process and sanctions.
- Developing overall privacy policies and procedures for the Plans.
- Establishing programs to audit and monitor Business Associates and internal privacy compliance such as where the Privacy Officer has actual knowledge (or has been apprised that someone in the Company has actual knowledge) of the failure of a Business Associate to comply with the HIPAA Privacy Rule pursuant to the Business Associate agreement.
- Keeping up to date on the latest privacy and security developments and federal and state laws and regulations that may affect the requirements under the Privacy Policy.
- Coordinate with the appropriate Company officers in directing the response to Breaches of Unsecured Protected Health Information.
- Coordinating with employer functions such as FMLA leave, drug testing and fitness-for-duty exams.
- Coordinating with the Security Officer to, among other things, review all system-related information throughout the networks of the members of the Company to ensure alignment between security and privacy practices and to act as a liaison to the Company's information systems departments.
- Cooperation with the HHS Office of Civil Rights, other legal entities and Company officers in any compliance reviews or investigations.

1.4 BUSINESS ASSOCIATE AGREEMENTS

POLICY/PROCEDURE

The Plan shall enter into an agreement with each entity or person who is a Business Associate. The HIPAA Privacy Group may disclose PHI to a Business Associate and may allow that Business Associate to create or receive PHI for or on behalf of the Plan **if, and only if**, the Plan and the Business Associate have entered into a Business Associate Agreement that is in a form substantially similar to the form provided in the Forms and Notices section of the Privacy Policy. The Plan is not required to enter into a Business Associate Agreement with a health care provider prior to disclosing information to such health care provider relating to the treatment of an individual.

Business Associate Agreements shall include satisfactory assurances from each Business Associate, respectively, that it shall make reasonable efforts to ensure that all uses and disclosures of PHI shall be made only in accordance with the terms and conditions of the Business Associate agreement, or as otherwise required under the HIPAA Privacy Rule and the HIPAA Security Rule.

A copy of the Business Associate agreement, executed by all parties, shall be maintained pursuant to the Record Retention and Documentation Policy.

If no Business Associate Agreement is on file, the HIPAA Privacy Group may not disclose any PHI to the Business Associate until such an agreement is on file. If the HIPAA Privacy Group is unable to obtain an executed Business Associate agreement from the Business Associate, the HIPAA Privacy Group may not disclose any PHI to the Business Associate.

To the extent that the Plan or a member of the HIPAA Privacy Group has actual knowledge of a violation of any Business Associate Agreement, the HIPAA Privacy Rule or the HIPAA Security Rule, the Company shall, on behalf of the Plan, take reasonable steps to ensure that the breach is cured. If the breach is not cured, the Business Associate Agreement shall be terminated or, if termination is not feasible, the Plan shall report the violation to HHS. Absent actual knowledge, the HIPAA Privacy Group shall have no obligation to monitor the activities of Business Associates with respect to their compliance with the Privacy Policy, the HIPAA Privacy Rule or the HIPAA Security Rule.

1.5 USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION AUTHORIZATION IS REQUIRED/NOT REQUIRED

POLICY

Subject to the exceptions described below, the Plan shall not use or disclose PHI unless it first obtains a valid authorization from the individual to whom the PHI relates (or his or her Personal Representative), in the form provided in the Forms and Notices section of the Privacy Policy. When the Plan receives a valid authorization, the use and disclosure of the PHI shall be made according to the terms of the authorization.

Exceptions to Authorization Requirement. The members of the HIPAA Privacy Group may use or disclose PHI without first obtaining an authorization and without providing the individual with the opportunity to agree or object under the following circumstances:

- Disclosure to the individual about whom the PHI relates.
- Use or disclosure made to facilitate Treatment, Payment or Health Care Operations.
- Inadvertent use or disclosure incident to a permitted use or disclosure.
- Disclosure to a public health authority.
- Disclosures about victims of abuse, neglect or domestic violence.
- Uses and disclosures for health oversight activities.
- Uses and disclosures for judicial or administrative proceedings.
- Disclosures for law enforcement purposes.
- Uses and disclosures about decedents.
- Uses and disclosures for cadaveric organ, eye or tissue donation purposes.
- Uses and disclosures for research purposes.
- Uses and disclosures to avert a serious threat to health or safety.
- Uses and disclosures for specialized government functions.
- Disclosures authorized by and to the extent necessary to comply with laws relating to workers' compensation and similar programs.
- Disclosure required by law, or otherwise permitted under the HIPAA Privacy Rule without an authorization.

Notwithstanding anything in this policy to the contrary, the Plan must receive a separate authorization from the individual prior to using or disclosing Psychotherapy Notes, except in certain situations permitted under the HIPAA Privacy Rule.

If the Plan needs to make a use or disclosure that requires an authorization, it shall use the appropriate authorization provided in Forms and Notices section below. The authorization shall not be valid past the date that the Plan received notice that the authorization has been revoked.

Note, that, while the use or disclosure described above may not require an authorization, the HIPAA Privacy Rule may contain additional requirements for each of the items listed above.

PROCEDURE

1. When a member of the HIPAA Privacy Group receives a request for PHI, he or she shall verify the identity of the requestor in accordance with the Verification Policy.
2. Prior to using or disclosing PHI, the HIPAA Privacy Group shall determine whether an authorization is required to make such use or disclosure pursuant to this policy and the HIPAA Privacy Rule. See

also the section entitled Disclosures to Personal Representatives, Individuals, Family Members and Friends.

3. If the use or disclosure requires neither an authorization nor an opportunity for the requesting individual to disagree or object to the use or disclosure, a member of the HIPAA Privacy Group shall refer to the Privacy Policy or the HIPAA Privacy Rule dealing with the type of use or disclosure at issue and follow the appropriate procedure for making that use or disclosure.
4. If authorization is required, the member of the HIPAA Privacy Group handling the request shall confirm receipt of an authorization (in the form required under this policy) and confirm whether the authorization is valid under the Privacy Policy and the HIPAA Privacy Rule.
5. When it is determined that the authorization is valid, the HIPAA Privacy Group may then use or disclose the Protected Health Information in accordance with the authorization.
6. If applicable, the HIPAA Privacy Group shall document the use or disclosure in accordance with the Record Retention and Documentation Policy.
7. If a valid authorization is not received, the HIPAA Privacy Group shall not use or disclose the Protected Health Information.

1.6 DISCLOSURES OF PROTECTED HEALTH INFORMATION TO THE COMPANY

POLICY

In general, the Plan may not disclose Protected Health Information to the Company. In addition, the Plan may only disclose Protected Health Information to a plan sponsored by the Company (other than the Plan) if it first receives an authorization from the individual. If possible, de-identified health information should be used instead of Protected Health Information. No authorization or de-identification of health information is necessary, however, if disclosure of Protected Health Information is authorized by and made to the extent necessary to comply with laws relating to workers' compensation and similar programs.

Permitted Disclosure. Notwithstanding the foregoing, at the Company's request, the Plan may disclose

- summary Health Information for the purpose of obtaining premium bids for providing health insurance under the Plan or for the purpose of modifying or terminating the Plan; or
- enrollment and disenrollment information

Requirements for Disclosure of Other Health Information. For a request for other Protected Health Information from the Plan other than as described above, the Plan shall not make the requested disclosure unless the Privacy Officer determines that the Plan documents have been amended to:

- Establish the permitted and required uses and disclosures of such information by the Company, provided that such permitted and required uses and disclosures may not be inconsistent with the HIPAA Privacy Rule or the HIPAA Security Rule.
- Provide that the Plan shall disclose Protected Health Information to the Company only upon receipt of a certification by the Company that the plan documents have been amended to incorporate the following provisions and that the Company agrees to:
 - Not use or further disclose the Protected Health Information other than as permitted or required by the Plan documents or as required by law.
 - Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that the Company creates, receives, maintains, or transmits on behalf of the Plan.
 - Ensure that any agents, including a subcontractor, to whom it provides Protected Health Information received from the Plan agree to the same restrictions and conditions that apply to the Company with respect to such information.
 - Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Company.
 - Report to the Plan any security incident, as defined under the HIPAA Security Rule, or any use or disclosure of the Protected Health Information that is inconsistent with the uses or disclosures provided for of which it becomes aware.
 - Make available Protected Health Information in accordance with an individual's right to access Protected Health Information under the HIPAA Privacy Rule.
 - Make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with the HIPAA Privacy Rule.
 - Make available the information required to provide an accounting of disclosures in accordance with the HIPAA Privacy Rule.

- Make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from the Plan available to the Secretary for purposes of determining compliance by the Plan the HIPAA Privacy Rule.
- If feasible, return or destroy all Protected Health Information received from the Plan that the Company still maintains in any form and do not retain any copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
- Ensure that the adequate separation between the Plan and the Company as required under paragraph (f)(2)(iii) of section 164.504 of the HIPAA Privacy Rule is established.

1.7 DISCLOSURES TO PERSONAL REPRESENTATIVES, INDIVIDUALS, FAMILY MEMBERS AND FRIENDS

POLICY/PROCEDURE: PERSONAL REPRESENTATIVES

In general, for purposes of the use and disclosure of Protected Health Information, the Plan shall treat a personal representative of an individual who is or has been a participant in the Plan in the same manner as the Plan would treat the individual. Prior to allowing a person to act as an individual's personal representative in connection with the Plan's use or disclosure of the individual's Protected Health Information, the Plan must determine if the individual is (A) an adult or emancipated minor; (B) an unemancipated minor; (C) deceased; or (D) a victim of abuse, neglect or endangerment. After making this determination, the Plan must follow the procedures described herein.

For all categories of individuals, the Plan must where appropriate obtain written documentation of a person's authority under applicable state law to act as the individual's personal representative before allowing the person to act as the individual's personal representative in connection with the use or disclosure of the individual's Protected Health Information.

If the Privacy Officer determines that the Plan should make the disclosure, then the Privacy Officer shall deliver the requested Protected Health Information to the personal representative. If the Privacy Officer determines that the disclosure should not be made, the Privacy Officer or his or her designee shall notify the person making the request.

Adults and Emancipated Minors. If the individual is an adult or emancipated minor, the Plan will treat a person who has authority under applicable state law to act on behalf of the individual in making decisions related to health care as such individual's personal representative with respect to Protected Health Information relevant to such personal representation.

Unemancipated Minors. The Plan will treat a parent, guardian or other person acting in loco parentis, as authorized under state law, as the personal representative of an unemancipated minor with respect to such minor's Protected Health Information. However, such person may not be an unemancipated minor's personal representative if, under any of the following three circumstances, the minor has the authority to act on his or her own behalf with respect to Protected Health Information:

- the minor consents to the health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the minor's personal representative;
- the minor may lawfully obtain the health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or
- a parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

In short:

- If, and to the extent, permitted or required by applicable state or other law, including case law, the Plan may disclose, or provide access to, Protected Health Information about an unemancipated minor to a parent, guardian or other person acting in loco parentis.

- Where prohibited under state law, the Plan may not disclose, or provide access to Protected Health Information about an unemancipated minor to a parent, guardian or other person acting in loco parentis.
- The Plan may provide or deny access under the Privacy Policy to a parent, guardian or other person acting in loco parentis who is not the personal representative, if there is no applicable access provision under state law, the decision is consistent with state law, and the decision is made by a licensed health care professional in the exercise of professional judgment.

Deceased Individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or the individual's estate, the Plan will treat such person as a personal representative with respect to Protected Health Information relevant to such personal representation.

Abuse, Neglect, Endangerment Situations. Notwithstanding state law or any requirement of the Privacy Policy to the contrary, the Plan may elect not to treat a person as the personal representative of an individual if

- the Plan 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
- the Privacy Officer decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Review against applicable state law. This section of the Privacy Policy will be administered in accordance with state law in that the HIPAA Privacy Rule may not be construed to preempt any state law to the extent that it authorizes or prohibits disclosure of Protected Health Information about a minor to a parent, guardian, or person acting in loco parentis of such minor.

POLICY/PROCEDURE: INDIVIDUALS, FAMILY MEMBERS AND FRIENDS

The Plan shall not disclose Protected Health Information to the individual, a family member or a close personal friend of the individual, except as required or permitted below.

Disclosures to Individuals. The Plan will disclose an individual's own Protected Health Information to the individual when requested by the individual, except information compiled in reasonable anticipation of or use in legal proceedings, Psychotherapy Notes, or clinical lab tests or lab results that fall under the Clinical Laboratory Improvements Amendments of 1988, 42 C.F.R. 493.3(a)(2).

Disclosures to Friends and Family Members. The Plan will only disclose an individual's Protected Health Information to another person if the Plan has a written authorization from that individual permitting it to make such disclosure. Under limited circumstances the Plan will disclose Protected Health Information to a family member, close personal friend, or other person identified by the individual without authorization. Such disclosure is limited to Protected Health Information that is directly relevant to that person's involvement with the individual's care or payment for health care, and where at least one of the following conditions are met:

- The individual agrees to the disclosure.
- The individual had an opportunity to agree or object to the disclosure and did not object.

- Based on professional judgment and the circumstances, it can reasonably be inferred that the individual did not object to the disclosure.
- If the individual was not available to agree or object, or cannot agree or object due to the Individual's incapacity (for example, in an emergency), but the disclosure is in the Individual's best interest.

Opportunity to object, for these purposes, means the individual was present or otherwise available prior to the disclosure and had the capacity to make health care decisions.

The Plan also may use or disclose Protected Health Information to notify or assist in the notification of a family member, personal representative, another person responsible for the individual's care, or a disaster relief organization, of the individual's location, condition, or death provided one of the conditions above is satisfied.

1.8 DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS

POLICY

The Plan may disclose Protected Health Information during the course of a judicial or administrative proceeding

- in response to an order of a court or administrative tribunal, OR
- in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal IF
 - the Plan receives “satisfactory assurances” from the party seeking the Protected Health Information that such party has made reasonable efforts to ensure that the individual to whom the requested Protected Health Information relates has been given notice of the request, OR
 - the Plan receives “satisfactory assurances” from the party seeking the Protected Health Information that reasonable efforts have been made by the party seeking the Protected Health Information to secure a “qualified protective order.”

Satisfactory Assurances of Reasonable Efforts to Notify. The Plan has received “satisfactory assurances” from the party requesting the Protected Health Information that such party has made reasonable efforts to ensure that the individual is notified of the request IF the Plan receives a written statement and supporting documentation demonstrating that: (1) the requesting party has made a good faith attempt to provide written notice to the individual (or, if the individual’s location is unknown, to mail a notice to the individual’s last known address); (2) the notice included sufficient information about the litigation or proceeding in which the Protected Health Information is requested to permit the individual to raise an objection with the court or administrative tribunal; and (3) the time for the individual to raise objections with the court or administrative tribunal have elapsed and no objection was filed or any objection filed has been resolved and disclosure of the Protected Health Information is consistent with the resolution.

Satisfactory Assurances of Reasonable Efforts to Obtain a Qualified Protective Order. The Plan has received “satisfactory assurances” from the party requesting the Protected Health Information that reasonable efforts have been made to secure a “qualified protective order” if the Plan receives a written statement and supporting documentation demonstrating that: (1) the parties to the dispute giving rise to the request for Protected Health Information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or (2) the party seeking the Protected Health Information has requested a qualified protective order from such court or administrative tribunal.

A “qualified protective order” is an order from a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (1) prohibits the parties from using or disclosing the Protected Health Information for any purpose other than the litigation or administrative proceeding for which it was sought; and (2) requires the return to the Plan or the destruction of the Protected Health Information, including all copies, at the end of the litigation or administrative proceeding.

PROCEDURE

1. If the request is a court or administrative tribunal order, the Privacy Officer shall disclose the requested Protected Health Information and document the disclosure pursuant to the Record Retention and Disclosure Policy.
2. If the request is a subpoena or discovery request that is not accompanied by a court or administrative tribunal order, the Privacy Officer shall determine whether there is either satisfactory assurances that the requesting party has made reasonable efforts to notify the individual about whom the Protected Health Information relates or satisfactory assurances that the requesting party has made reasonable efforts to secure a qualified protective order.
3. If such satisfactory assurances have been received, the Privacy Officer shall disclose the requested Protected Health Information and document the disclosure accordingly.
4. If such satisfactory assurances have not been made, the Privacy Officer shall contact an attorney (if the Privacy Officer is not an attorney) to determine the Plan's obligations under the subpoena. If, after consulting with an attorney, the Privacy Officer determines that the request should be denied, the Privacy Officer will notify the person who issued the subpoena and places the subpoena or discovery order in the Plan's files relating to denied requests for Protected Health Information.

1.9 USES AND DISCLOSURES REQUIRED BY LAW

POLICY

The HIPAA Privacy Group shall use and disclose Protected Health Information when such use or disclosure is required by law, and shall limit such use or disclosure to the relevant requirements of such law.

A use or disclosure is “required by law” under the Privacy Policy when a mandate contained in law compels an entity to make a use or disclosure of Protected Health Information that is enforceable in a court of law. Examples include disclosure made:

- To a government authority, including social or protective services authorities, about an individual that the Plan reasonably believes is a victim of abuse, neglect or domestic violence.
- In the course of a judicial or administrative proceeding in response to an order of a court or an administrative body or in response to a court ordered subpoena, discovery request or other lawful process.
- To a law enforcement official for certain law enforcement purposes.
- Pursuant to statutes or regulations that require the production of information.

1.10 VERIFICATION

POLICY

If the identity or authority of a person requesting Protected Health Information is not known to the HIPAA Privacy Group, the HIPAA Privacy Group shall verify the identity and authority of the person prior to providing any access to or disclosing the Protected Health Information to the person making the request. As necessary under the HIPAA Privacy Rule, and as part of the process of verifying the identity and authority of an individual, the HIPAA Privacy Group shall receive all documentation, statements or representations necessary as a condition of the disclosure.

PROCEDURE

Verification of Identity. The HIPAA Privacy Group shall verify the identity of the person requesting the Protected Health Information.

- Where the disclosure is conditioned on particular documentation or representation from the requesting individual, the HIPAA Privacy Group may rely, if such reliance is reasonable, based on the face of the documents or representations themselves. The member of the HIPAA Privacy Group conducting such verification shall examine the HIPAA Privacy Rule for situations where such conditions exist and apply them accordingly.
- If the person making the request is a public official, the identity of that person may be verified by
 - viewing an agency identification badge or other proof of government employment;
 - if the request is received in writing, the request is on government letterhead; or
 - if the disclosure is to a person acting on behalf of a public official, a statement on government letterhead which states that the person is acting on behalf of a public official, or other documentation of the relationship between the individual making the request and the public official for whom the request is being made.

Verification of Authority. The HIPAA Privacy Group shall verify the authority of the person making the request to receive the Protected Health Information.

- If the request is made by a public official, authority may be verified
 - by a written or oral statement of legal authority; or
 - by viewing the warrant, subpoena, order or other legal process pursuant to which the request is being made.

If required, the appropriate member of the HIPAA Privacy Group shall document the basis for the verification and the disclosure pursuant to Record Retention and Documentation Policy.

1.11 NOTICE OF PRIVACY PRACTICES

POLICY

It is a violation of the Privacy Policy to use or disclose Protected Health Information in a manner which is inconsistent with the Notice of Privacy Practices then in effect. (The Notice of Privacy Practices is set forth in the Forms and Notices section of the Privacy Policy.).

PROCEDURE

In the event that the Privacy Officer believes or is notified that the privacy practices contained in the Notice of Privacy Practices should be changed for any reason, the Privacy Officer shall review the current Notice of Privacy Practices and the Privacy Policy and make any changes the Privacy Officer, in consultation with the Security Officer, determines to be necessary and appropriate. In that case, the Privacy Officer must revise the Privacy Policy in accordance with the Amending the Privacy Policy section and revise and redistribute the Notice of Privacy Practices in accordance with the applicable procedures set forth below.

The Privacy Officer shall cause the Notice of Privacy Practices to be distributed to individuals at all times and in the manner required under the HIPAA Privacy Rule. Unless the HIPAA Privacy Rule provides otherwise:

- All individuals that participate in the Plan (named insured) shall be provided a Notice of Privacy Practices on or before the date the Plan first becomes subject to the HIPAA Privacy Rule, and thereafter as a standard part of enrollment in the Plan, as required under the HIPAA Privacy Rule.
- The Notice of Privacy Practices will be included in the Plan's enrollment materials for new enrollees.
- In the event of a material change in the Privacy Policy, all individuals then covered under the Plan shall be provided with a revised Notice of Privacy Practices within 60 days of the material revision. The Plan may post the change or its revised notice on its web site by the effective date of the material change, and provide the revised notice, or information about the material change and how to obtain the revised notice in its next annual mailing to individuals then covered by the plan. If the Plan does not post its notice on a web site, then it must provide the revised notice or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.
- Every three years, the Privacy Officer shall notify all individuals then covered of the availability of the Notice of Privacy Practices and how to obtain it.
- In the event the Company or Plan maintains a website describing information regarding Plan benefits, the Notice of Privacy Practices shall be prominently displayed on such site.

1.12 DE-IDENTIFIED INFORMATION

POLICY

If Protected Health Information is converted by the HIPAA Privacy Group to “de-identified” information in accordance with the Privacy Policy and the HIPAA Privacy Rule, the converted information will no longer be subject to the Privacy Policy, the HIPAA Privacy Rule or the HIPAA Security Rule. Protected Health Information is converted into de-identified information if: (1) certain specific identifiers are removed; and (2) the Plan does not know that the remaining information can be used to identify an individual (either alone or in combination with other information).

PROCEDURE

To convert Protected Health Information to de-identified information, the following identifiers that relate to individuals, their relatives, other household members or employers must be removed:

- Names of individuals.
- Geographic units -- all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geo-codes. However, the initial three digits of a zip code may be used if, according to Census Bureau data, the geographic unit formed by combining all Zip Code Tabulation Areas (ZCTAs) with the same three initial digits has more than 20,000 people, and the initial three digits of all such geographic units with 20,000 or fewer people are changed to 000. Results of the 2000 Census indicate that only 17 three-digit ZCTAs have fewer than 20,000 people.
- Dates -- any month or day directly related to an individual, including birth date, admission date, discharge date and date of death. However, listing an individual's age is broad enough to be allowed in de-identified information (subject to the exception for individuals age 90 or older described below).
- Ages -- all those over 89 and any combination of month, day or year that reveals an individual's age to be over 89, because nonagenarians are relatively rare. However, ages and identifying dates (month, day and year) of several individuals may be aggregated into a single category of age 90 or older.
- Telephone numbers.
- Fax numbers.
- E-mail addresses.
- SSNs.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web universal resource locators (URLs).
- Internet protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic or code, except a re-identification code.

1.13 [RESERVED]

2. POLICIES REGARDING THE RIGHTS OF INDIVIDUALS UNDER THE HIPAA PRIVACY RULE

2.1 ACCESS TO PROTECTED HEALTH INFORMATION

POLICY/PROCEDURE

Generally, every individual has the right to inspect and obtain a copy of his/her own Protected Health Information that is maintained by the Plan in accordance with the following procedures:

1. All requests for access to Protected Health Information shall be made by an individual or his or her personal representative and shall be made in writing to the HIPAA Privacy Group using the form attached in the Forms and Notices section of the Privacy Policy.
2. The HIPAA Privacy Group shall respond to all requests for access within 30 days of receipt of the request. If the HIPAA Privacy Group is unable to respond within either time frame, it shall seek an extension of time to respond by notifying the requestor (within the respective time frames mentioned in the preceding sentence) in writing of the reasons for the delay and the date it will make its determination. The extension may be made only one time and not for longer than 30 days.
3. A request for access to Protected Health Information may be denied if
 - the Protected Health Information requested is Psychotherapy Notes;
 - the Protected Health Information requested was compiled in reasonable anticipation of a civil, criminal or administrative action (e.g. lawsuits and similar proceedings);
 - the Protected Health Information requested is subject to the Privacy Act, 5 USC Sec. 552; or
 - the Protected Health Information requested was obtained from someone other than a health care provider under a promise of confidentiality and the access would likely reveal the source.

If it is determined under this policy that access to the requested Protected Health Information must be denied because of one or more of the reasons set forth above, that determination shall not be subject to review at the request of the individual or his or her personal representative.

4. In certain cases, the determination to deny access to Protected Health Information may be reviewed by the individual or his or her personal representative. Those situations, as set forth in the HIPAA Privacy Rule (45 CFR 164.524(a)(3)), are incorporated herein by reference. In those cases, the HIPAA Privacy Group shall provide for a review of the determination pursuant to the HIPAA Privacy Rule.
5. If it is determined under this policy that access to the requested Protected Health Information must be provided to the individual, the HIPAA Privacy Group shall notify the individual or his or her personal representative in writing that the request has been granted and provide the Protected Health Information to the requesting individual or his or her personal representative at a convenient time or location and in the form requested, unless such form is not readily producible and then in hard copy or another form mutually agreeable to the individual and the HIPAA Privacy Group.
6. The HIPAA Privacy Group may impose a reasonable, cost-based, fee which shall include only the cost of: (i) copying the Protected Health Information, including the supplies and labor involved; (ii)

postage for mailing the Protected Health Information; and (iii) if agreed to with the requesting individual the cost of preparing an explanation or summary of the Protected Health Information.

7. In any case in which access to the requested Protected Health Information is denied, the HIPAA Privacy Group shall, to the extent possible, provide access to any other Protected Health Information requested that is not part of the Protected Health Information that the Plan has grounds to deny access. With respect to the Protected Health Information to which the Plan denies access, the HIPAA Privacy Group shall notify the requesting individual or his or her personal representative of the denial in a writing that states
 - the basis for the denial;
 - if applicable, a statement that the individual may have the right to have a licensed health care professional, chosen by the Plan, review the decision to deny access to the Protected Health Information including a description of how the individual may exercise such review rights;
 - the procedure by which the requesting individual or his or her personal representative may file a complaint with the Plan and the title and telephone number of the person with whom the complaint can be filed; and
 - the procedure by which the requesting individual or his or her personal representative may file a complaint with the Plan or the Secretary of Health and Human Services.
8. If the denial of access is subject to review under number 4 above and the requesting individual or his or her personal representative requests a review, the HIPAA Privacy Group shall appoint a licensed health care professional not involved in the original decision to deny access to review the request. The HIPAA Privacy Group and the requesting individual or his or her personal representative are bound by the determination made by the reviewing health care professional.
9. The HIPAA Privacy Group shall document the Designated Record Sets that are subject to review and the titles of the persons or offices responsible for receiving and processing requests for access.

2.2 AMENDMENTS TO PROTECTED HEALTH INFORMATION

POLICY/PROCEDURE

Individuals in the Plan have the right to request that the Plan amend Protected Health Information or a record about the individual in a Designated Record Set for so long as such Protected Health Information or record exists in a Designated Record Set. The Plan may only deny the individual's request to have his or her Protected Health Information or a record amended if

- the Protected Health Information or record was not created by the Plan, unless the individual provides a reasonable basis to believe that the originator of the Protected Health Information is no longer available to amend it,
- it is not part of a Designated Record Set,
- the individual does not have the right to inspect the Protected Health Information which he or she is requesting to have amended, as set forth in Access to Protected Health Information policy, or
- the Protected Health Information is accurate and complete.

All requests for an amendment of Protected Health Information must be made by the individual or his or her personal representative and be in writing to the HIPAA Privacy Group using the form attached in the Forms and Notices section of the Privacy Policy. The request shall include a reason that supports the requested amendment. If the amendment request applies to Protected Health Information not contained in the Plan's Designated Record Set and is not otherwise in the possession of the Company or the Plan, no amendment shall be required.

The Plan, through the HIPAA Privacy Group, shall attempt to act on every request for an amendment within 60 days of receiving the request in accordance with the following:

1. If the Plan grants the requested amendment:

- The Plan shall make the appropriate amendment to the Protected Health Information or record that is the subject of the request by identifying the Protected Health Information or records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
- The Plan shall notify the individual that the amendment was accepted and shall obtain from the individual the identification of those persons with whom the amendment should be shared, and authorization to share such amendment.
- The Plan shall make reasonable efforts to inform and provide the amendment within a reasonable time to: (i) persons identified by the individual as having received Protected Health Information about the individual and needing the amendment; and (ii) persons, including Business Associates, that the Plan knows have Protected Health Information which is the subject of the amendment and that may have relied, or could foreseeably rely, on the Protected Health Information to the detriment of the individual.

2. If the Plan denies the requested amendment:

- The Plan shall provide a written denial to the individual which contains
 - the basis for the denial,
 - a statement that the individual has the right to submit a written statement disagreeing with the denial and how the individual may file such a statement,

- a statement that if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with future disclosures of the Protected Health Information that is the subject of the request, and
 - a description on how the individual may file a complaint with the Plan in accordance with the Complaint Policy or to the Secretary of HHS. This description shall contain the name or title, and telephone number of the Plan's contact person.
- The individual or his or her personal representative may file a written statement of reasonable length setting forth the basis for his or her disagreement with the denial of the request for amendment.
 - If the individual files a written statement disagreeing with the denial of the request for amendment, the Plan may prepare a written rebuttal to the individual's statement of disagreement. The Plan shall provide a copy of the rebuttal to the individual.
 - The Plan shall, as appropriate, identify the record or Protected Health Information in the Designated Record Set that is the subject of the disputed amendment and append, or otherwise link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any, to the Designated Record Set.
 - In the case of future disclosures of Protected Health Information with respect to which the individual filed a statement of disagreement, the Plan shall include the material appended as described in the preceding paragraph or, as the Plan may elect, an accurate summary of such information. If the individual submitted no statement of disagreement, the Plan shall, only at the request of the individual, include a copy of the request for amendment and statement of denial, or a summary thereof, with disclosures of the Protected Health Information to which the amendment relates. If the future disclosure is made using a standard transaction that does not permit the disclosure of additional material to be included with the disclosure, the Plan shall separately transmit the appended information to the recipient of the standard transaction.
- 3. If the Plan is unable to act on the requested amendment within 60 days of receipt, the Plan shall inform the individual within the 60-day period by providing a written notice containing the reasons for the delay and the date on which the Plan will complete its action on the request. The Plan may not extend the time for action by more than 30 days and may extend the time for action only once for each request for amendment received.
- 4. If the Plan is informed of an amendment to an individual's Protected Health Information by another plan, the Plan shall amend the individual's Protected Health Information in accordance with the procedure by which the Plan amends Protected Health Information if a request for amendment is accepted.
- 5. The Plan shall document the title of the person or office responsible for receiving and processing requests for amendments by an individual and shall retain such documentation in accordance with the Record Retention and Documentation Policy.

2.3 COMPLAINTS

POLICY

The HIPAA Privacy Group shall receive, document and investigate every complaint that an individual makes regarding the Privacy Policy or use or disclosure of his or her Protected Health Information. Any such complaint shall be filed with the Privacy Officer or Security Officer, as appropriate, or such person or persons who may be designated by the Privacy Officer or Security Officer for this purpose (the "Complaint Investigator").

Complaints shall be made in writing to the HIPAA Privacy Group by the individual or his or her personal representative. A form for complaints is attached in the Forms and Notices section of the Privacy Policy.

All complaints shall be investigated. If it is determined that there has been a violation of the HIPAA Privacy Rule, the HIPAA Security Rule, or the Privacy Policy, the Privacy Officer or Security Officer, as appropriate, shall take any action required under the Mitigation Policy, the Sanctions Policy, the HIPAA Privacy Rule or the HIPAA Security Rule, as applicable.

At no time will a workforce member who is the subject of a complaint be the same person in charge of investigating the complaint.

PROCEDURE

1. The Plan, through its Complaint Investigator, shall accept only written complaints.
2. The Complaint Investigator shall document the complaint process and all actions taken with respect thereto according to the Record Retention and Documentation Policy.
3. The Complaint Investigator shall review all available information relating to the use or disclosure of the complaining individual's Protected Health Information, including all written documentation relating to the use and disclosure of such Protected Health Information.
4. If the Privacy Officer or the Security Officer, as applicable, agrees with the Complaint Investigator's determination, the Officer shall sanction the workforce member responsible for the inappropriate use or disclosure of the Protected Health Information in accordance with the Sanction Policy. If necessary, the Officer shall take steps to mitigate the effects of an inappropriate use or disclosure in accordance with the Mitigation Policy. The Officer shall document the action taken and place all information relating to the individual's complaint in the Complaint File.
5. If Complaint Investigator determines that the complaint has no merit, the investigation made is documented and placed in the Complaint File.
6. In the event that the complaint is about the Complaint Investigator and/or the Security Officer, the complaint shall be handled by Privacy Officer. In the event that the complaint is about the Privacy Officer, the complaint shall be handled by the Security Officer. In the event that the complaint is about the Privacy Officer and the Security Officer, the complaint shall be handled by the **Corporate Director, Human Resources** according to this Complaint Policy.

2.4 CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION

POLICY

An individual or his or her personal representative may request that the Plan communicate Protected Health Information to the individual by alternative means or at alternative locations. The Plan acting through members of the HIPAA Privacy Group shall accommodate all such requests that are reasonable in the discretion of the Privacy Officer.

Any request for confidential communications shall be made in writing to the HIPAA Privacy Group. A form for such request is attached in the Forms and Notices section of the Privacy Policy.

A member of the HIPAA Privacy Group shall accommodate such a request only after the individual provides an alternative address or method of contact and, when necessary and appropriate, information on how payment will be handled. The Plan shall not require the individual to explain why he or she is seeking such an accommodation.

PROCEDURE

1. If the request is determined to be reasonable, within the discretion of the Privacy Officer, and the Plan is capable of accommodating the request, the Privacy Officer or his or her designee shall:
 - notify individual or his or her personal representative that reasonable accommodation will be made;
 - if necessary and appropriate, discuss how payment will be handled while accommodation is being made;
 - if not already included in the individual's request, ask the individual to provide an alternative address or method of contact;
 - document the location at which or the manner by which Protected Health Information is to be communicated and place the documentation in the individual's Protected Health Information file; and
 - inform relevant Business Associates of the request and the alternate means and/or locations of providing confidential communications.
2. If the Privacy Officer determines that the request is unreasonable and the Plan is unable to make such an accommodation, the Privacy Officer shall notify the individual or his or her personal representative of the decision.

2.5 DOCUMENTING DISCLOSURES AND ACCOUNTINGS

POLICY

Generally, within 60 days of receiving a request from an individual or his or her personal representative, the Privacy Officer, or his or her designee, shall provide an accounting of all documented disclosures of Protected Health Information that have been made during the period for which the accounting was requested. The accounting period cannot exceed the six (6) years prior to the date on which the request for an accounting was received. The accounting period is three (3) years in the case of electronic health records pertaining to treatment, payment, or health care operations. An accounting need not include any disclosure that the Plan is not required to document under the HIPAA Privacy Rule. All requests to account for disclosures of Protected Health Information shall be in writing to the HIPAA Privacy Group. A form for such requests is attached in the Forms and Notices section of the Privacy Policy.

PROCEDURE – DOCUMENTING DISCLOSURES

1. Except as otherwise provided in paragraph 3 below, when Protected Health Information is disclosed, the disclosure shall be recorded in the Protected Health Information Disclosure Log, the form for which is contained in the Forms and Notices section of the Privacy Policy.
2. Every record of a disclosure shall include:
 - The date the disclosure was made.
 - The name and, if known, the address of the entity or person who received the Protected Health Information.
 - A brief description of the Protected Health Information disclosed.
 - A brief statement of the purpose for the disclosure which reasonably describes the basis on which the disclosure was made or a copy of the written request for disclosure.
3. A disclosure need not be documented if the disclosure was made for the following purposes:
 - To carry out Treatment, Payment or Health Care Operations, other than for electronic health records as described above).
 - To the individual about whom the Protected Health Information relates.
 - Incident to an otherwise permissible disclosure under the HIPAA Privacy Rule.
 - Pursuant to an authorization given by the individual.
 - For national security reasons or intelligence purposes.
 - To a correctional facility or to law enforcement officials.
 - As part of a limited data set.
 - Prior to the compliance date of the HIPAA Privacy Rule for the Plan.

PROCEDURE – ACCOUNTING FOR DISCLOSURES

1. The Privacy Officer, or his or her designee, shall, to the extent possible, prepare the requested accounting within 60 days of receiving the request. The accounting may cover either (i) disclosures made by the Plan and its business associates or (ii) disclosures made by the Plan along with a list of all business associates acting on behalf of the Plan including their contact information.
2. The accounting prepared shall include the following information relating to all documented disclosures made during the accounting period, which period may not exceed the 6 years (3 years in

the case of electronic health records) prior to the date on which the request for an accounting was received:

- The date of the disclosure.
 - The name and, if known, the address of the person to whom the disclosure was made.
 - A brief description of the Protected Health Information which was disclosed.
 - A brief statement of the purpose for the disclosure which reasonably sets forth the basis upon which the disclosure was made.
3. If the requested accounting cannot be provided within 60 days of receiving the request, the Privacy Officer may extend the time period for providing the accounting by 30 days provided the Privacy Officer, or his or her designee, during the initial 60-day period, notifies the requestor of the reasons for the delay and indicates when the accounting shall be provided.
 4. If during the same 12-month period the same individual or his or her personal representative makes more than one request for an accounting, the Privacy Officer may impose a reasonable cost-based fee with respect to each request provided that the Privacy Officer provides the individual or his or her personal representative with: (i) advance notice of the fee; and (ii) an opportunity to withdraw the request to avoid or reduce the fee. The fee shall be calculated in the same manner as under the Access to Protected Health Information Policy.
 5. The Privacy Officer shall suspend the requestor's right to an accounting if the Plan is notified by a health oversight committee or law enforcement agency that making an accounting would impede such agency's activities.
 - If notified in writing, the right to an accounting shall be suspended for the period set forth in the notification from the agency.
 - If notified orally, the right to an accounting shall be suspended for no longer than 30 days, unless the appropriate agency subsequently provides notice in writing.
 - The Privacy Officer shall document this suspension accordingly, and inform the requestor of such suspension.

2.6 REQUESTING RESTRICTIONS ON USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

POLICY

The Plan shall allow any individual or his or her personal representative to request a restriction on the uses and disclosures of Protected Health Information made on behalf of the Plan about the individual to carry out Treatment, Payment or Health Care Operations. Additionally, the Plan shall allow any individual or his or her personal representative to request a restriction on the disclosure of Protected Health Information about the individual to a family member, other relative, close personal friend or other person designated by the individual relating to such person's involvement with the individual's care or payment for the individual's health care or to inform a family member, other relative, close personal friend or other person responsible for the care of the individual about the individual's location, general condition or death.

Any request for a restriction shall be made in writing to the HIPAA Privacy Group. A form for such requests is attached in the Forms and Notices section of the Privacy Policy.

The Privacy Officer is not obligated to agree to a requested restriction.

If the Privacy Officer, on behalf of the Plan, agrees to any requested restriction, the Protected Health Information shall not be used or disclosed in violation of the restriction, except to the extent such Protected Health Information is necessary to provide the emergency treatment to the individual or other purposes permitted under the HIPAA Privacy Rule, despite the existence of a restriction to the contrary. An approved restriction may only be terminated pursuant to the HIPAA Privacy Rule.

PROCEDURE

1. The HIPAA Privacy Group shall review and respond to all restriction requests. Such responses shall be subject to review by the Privacy Officer. All cases denying the restriction request must be approved by the Privacy Officer.
2. Following a review of a restriction request, the Privacy Officer or his designee shall inform the individual or his or her personal representative whether the Plan has agreed to the restriction requested.
3. If the restriction request is approved, the Privacy Officer shall maintain a copy of the request for restriction in the individual's Protected Health Information file and in the "Active Restriction File." Notation shall be made where necessary, electronic or otherwise, to ensure that the restriction is followed.
4. If the restriction request is not approved, the Privacy Officer shall maintain a copy of the request for restriction in the individual's Protected Health Information file.
5. If the Privacy Officer agrees to a restriction, the individual's Protected Health Information may not be used or disclosed in violation of the restriction, except as provided in the Privacy Policy.

2.7 GENETIC INFORMATION NONDISCRIMINATION ACT

In compliance with the Genetic Information Nondiscrimination Act, the Plan does not discriminate against any Plan participant or applicant on the basis of the individual's genetic information. Accordingly, with respect to health coverage determinations, the Plan shall not use genetic information as a basis for determining eligibility or setting premiums. Further, the Plan shall not use or disclose genetic information for underwriting purposes to the extent prohibited by law.

Additionally, in compliance with the HIPAA Final Rule, the Plan will protect genetic information in the same manner as PHI in accordance with the policies and procedures contained in this Manual. Where the term PHI appears in this Manual, it should be interpreted to include genetic information.

The term "genetic information" is defined in the Genetic Information Nondiscrimination Act, which defines "genetic information" to mean, with respect to any individual, information about: (1) such individual's genetic tests; (2) the genetic tests of family members of such individual; and (3) the manifestation of a disease or disorder in family members of such individual (i.e., family medical history). The term also includes any request for, receipt of, genetic services, or participation in clinical research which includes genetic services by such individual or family member of such individual. Genetic information does not include the sex or age of any individual.

3. POLICIES REGARDING ELECTRONIC PROTECTED HEALTH INFORMATION

3.1 IN GENERAL

The Plan will secure and electronic Protected Health Information (also known as e-PHI), if any, that it creates, receives, maintains, or transmits in accordance with this Privacy Policy, the HIPAA Security Rule and applicable state law. The Plan, however, generally does not create, receive, maintain, or transmit e-PHI. Instead, e-PHI generally is handled with respect to the Plan by Business Associates, third party administrators, insurance carriers, brokers and/or other service providers. However, to the extent the Plan does create, receive, maintain, or transmit e-PHI, it is the Plan's policy to implement and enforce the provisions in the Privacy Policy and, in particular, this section. In general, this means that the Plan will:

- Ensure the confidentiality, integrity, and availability of all e-PHI the Plan creates, receives, maintains, or transmits;
- Protect against any security incidents;
- Protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted by the HIPAA Privacy Rule; and
- Ensure workforce compliance.

3.2 ADMINISTRATIVE SAFEGUARDS

The Plan generally does not create, receive, maintain, or transmit any e-PHI (other than enrollment and disenrollment information, summary health information, or information obtained pursuant to an authorization) because the Plan outsources most administrative functions to Business Associates and insurers. As a result, the Plan does not have specific procedures to address certain implementation specifications with respect to the following standards of the HIPAA Security Rule:

- Workforce Security
- Information Access Management
- Contingency Plan

However, the general policies and procedures outlined in this Privacy Policy have been determined to provide adequate safeguards. For example, see sections 1.1 and 6.3 which provide safeguards for, among other things, workforce security and clearance, and access and termination procedures.

3.2.1 SECURITY RISK ASSESSMENT, SECURITY MANAGEMENT AND EVALUATION

The Plan must conduct a risk analysis for the purpose of determining what security measures are appropriate. The Plan must therefore conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the e-PHI it holds. The tools provided in Sections 7.18 and 7.19 can should be used to assist in completing this step.

The Plan conducts assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the Plan periodically, as warranted by changes in environmental, technological, or operational conditions. To appropriately consider the potential vulnerabilities to the Plan's e-PHI, the Plan uses the following risk analysis strategy:

- Identify and document all e-PHI containing systems or applications (repositories),

- Identify the potential threats or vulnerabilities to each repository,
- Assign a level of risk to each e-PHI repository, and
- As appropriate, mitigate the risk to each e-PHI repository.

The risk analysis will consider all relevant losses that would be expected if the security measures were not in place. “Relevant losses” would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures. The degree of response is determined by the risks identified.

An e-PHI repository may be a database, spreadsheet, folder, storage device, document, or other form of electronic information. Because the Plan outsources all administrative and customer service functions to Business Associates and others, the Plan currently creates, receives, maintains, or transmits little, if any, e-PHI and therefore has few, if any, e-PHI repositories. Thus, the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by the Plan are negligible.

The Plan will perform periodic inventories at regular intervals to identify any e-PHI repositories and to ensure the risk analysis is up-to-date and accurate. The Plan will perform periodic technical and nontechnical evaluations of security compliance. Evaluations will be conducted in response to environmental or operational changes affecting the security of e-PHI. Existing policies and procedures shall be reviewed to determine if they are sufficient in light of such environmental and operational changes. The Plan will assess the need for a new evaluation based on changes to their security environment since their last evaluation, taking into consideration such issues as the adoption of new technology, or recognizing additional risks to the security of e-PHI.

Violations of the policies and procedures in this section will be handled through the Sanctions policy under this Privacy Policy.

3.2.2 APPOINTMENT AND DUTIES OF THE SECURITY OFFICER

The Company, on behalf of the Plan, shall appoint a Security Officer (and set forth such appointment in the Appendix to the Privacy Policy) to implement and oversee compliance with the requirements of the HIPAA Security Rule.

The Security Officer is responsible for enforcement of the HIPAA Security Rule including the development, implementation, and maintenance of the policies and procedures to meet the requirements of the HIPAA Security Rule as applicable to the Company and the Plan, developing employee training programs, and, except as otherwise provided in the Privacy Policy, serving as the designated decision maker for issues and questions involving interpretation of the HIPAA Security Rule, in coordination with the Privacy Officer and legal counsel. The Security Officer also is responsible for cooperating with the HHS Office of Civil Rights or Center for Medicare Services, other legal entities and Company officers in any compliance reviews or investigations concerning the HIPAA Security Rule.

3.2.3 SECURITY AWARENESS AND TRAINING

The Security Officer shall ensure that members of the HIPAA Privacy Group and other workforce members of the Company will be trained to the extent that the Security Officer or his or her designee determines the training is needed to ensure those workforce members understand the restrictions imposed by the Privacy Policy and the HIPAA Security Rule with regard to any responsibilities they are asked to perform on the Plan’s behalf.

Workforce awareness and training will include a description of what entities maintain e-PHI on the Plan's behalf, relevant provisions of the Privacy Policy and other applicable Company procedures, and all relevant names and contact information in the event that any workforce members require more detailed information or inadvertently or improperly access e-PHI. In addition, security awareness and training will include, in coordination with existing Company policy, periodic security reminders, procedures for protection from malicious software utilizing virus protection, user education in the importance of log-in monitoring procedures and how to report discrepancies, and user education in password management controls.

3.2.4 SECURITY INCIDENT PROCEDURES

The Plan must (i) identify and respond to suspected or known Security Incidents, (ii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Plan, (iii) document Security Incidents and their outcomes; and (iv) if the Security Incident involves the disclosure of PHI, conduct a risk assessment to determine the probability that PHI has been compromised and whether breach notification is required. In the event an employee or HIPAA Privacy Group member becomes aware of a suspected or actual Security Incident, he or she shall report the incident to his or her direct supervisor and the Security Officer immediately. Security Incidents shall be handled by the Security Officer in a manner similar to the procedure described in the Sanction section of the Privacy Policy. In the event the Company becomes aware of a Security Incident, it must follow the procedures outlined in this section and in the Data Breach Response Checklist contained in Section 7 of this Manual at 7.16, in coordination with other Company protocols that are at least as stringent.

As soon as the Security Officer learns of a Security Incident that may involve a Breach of Unsecured Protected Health Information, he or she shall coordinate with the Privacy Officer, General Counsel and designated human resources and IT members to take such actions as necessary and appropriate to respond. The group assembled by the Security Officer to respond to the incident shall act as quickly as possible to implement this policy which, at a minimum, shall include the following steps:

- investigating the nature and scope of the incident, which may include contact and coordinating with law enforcement, as appropriate;
- determining whether the incident constitutes a Breach of Unsecured Protected Health Information requiring notification;
- securing Protected Health Information from further unauthorized access, use, disclosure, modification or destruction;
- reviewing existing insurance policies for potential coverage of losses related to security incidents and contacting all insurance carriers, as appropriate;
- coordinating with the Legal and Public Relations department for counsel concerning breach response, if applicable;
- reasonably mitigating, to the extent practicable, harmful effects of the Breach that are known, which may include providing breach notification letters in accordance with applicable law and making a monitoring service available;
- notifying affected persons and federal and state agencies as soon as practicable and without unreasonable delay in the manner required under applicable law (see form notification in the Forms and Notices section);
- in accordance with the Record Retention and Documentation Policy, documenting the efforts to respond, the post-breach review of events and actions taken, if any, to make changes in Program;
- reviewing policies and procedures to determine whether modifications or additional policies and procedures are needed.

In the case of a Breach of Unsecured Protected Health Information, notification must be provided without unreasonable delay but in no case later than 60 days following discovery of breach, following a reasonable period to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individuals. Additionally, written notification by first-class mail is the general or default rule. However, individuals who affirmatively agree to receive notice by e-mail may be notified accordingly.

3.2.5 DATA BACK-UP PLAN

In coordination with the Company's IT Department, the Privacy and Security Officers will establish a backup process appropriate for the Plan's e-PHI. As appropriate, multiple copies of backup tapes should be kept off-site and in separate locations.

3.2.6 DISASTER RECOVERY AND EMERGENCY MODE PLAN

The Privacy Officer will appoint members of the HIPAA Privacy Group who will be required to access Company facilities in the event of a disaster to attempt to secure and recover e-PHI. The designated person(s) shall inform building owners/landlords and/or building security management of their access in the event of emergency. The designated person(s) shall be trained as appropriate to take essential steps to secure and safeguard e-PHI until more resources can reasonably and safely be made available. The Privacy and Security Officers shall maintain the phone number(s) of the person(s) designated under this policy.

3.3 PHYSICAL AND TECHNICAL SAFEGUARDS

The Plan generally does not create, receive, maintain, or transmit any e-PHI (other than enrollment and disenrollment information, summary health information, or information obtained pursuant to an authorization) because the Plan outsources all administrative functions to Business Associates and insurers. As a result, except as provided below, the Plan does not have specific procedures concerning physical and technical safeguards. However, the general policies and procedures outlined in this Privacy Policy have been determined to provide adequate safeguards.

3.3.1 DEVICE AND MEDIA CONTROLS

Whenever a HIPAA Privacy Group member removes Protected Health Information from a facility, or from its assigned storage location (such as when taking a portion of a paper file, or using a laptop, flash drive, CD or other transportable electronic device containing Protected Health Information), he or she shall maintain such item or equipment in a secure location, and use all necessary steps to maintain the privacy, security and integrity of the information pursuant to the Privacy Policy.

This policy applies to any "device or media," which refers to any form of equipment that can be used to store, access, transmit, process, modify or destroy Protected Health Information. Examples include: laptops, flash drives, CDs, external hard drives, cell phones, blackberries, personal data assistants, and so on. When any device or media is used in connection with Protected Health Information, the following guidelines shall apply:

- Protected Health Information may only be stored on Company provided device and media.
- Unless otherwise captured by the Company, the Security Officer shall maintain a log of the device or media assigned to each HIPAA Privacy Group member, and where feasible maintain a

log or otherwise track whether Protected Health Information is maintained on a particular device or media.

- In the event any device or media will be reused or reassigned for another purpose or by another workforce member who does not have access or a need to access to Protected Health Information stored on the device or media, such Protected Health Information shall be removed from reusable media before it is reused or reassigned. This process must be confirmed by the Security Officer.
- When no longer needed, all devices and media shall be disposed and destroyed pursuant to this Privacy Policy. Prior to any disposal or destruction, the appropriate member of the HIPAA Privacy Group, in consultation with appropriate Company personnel, shall determine the type of information maintained on the device and media and take into account any applicable record retention requirements.

3.3.2 ACCESS AND AUDIT CONTROLS

In order to support the safeguards concerning access provided elsewhere in the Privacy Policy, the following guidelines, coordinated through the Company IT Department, shall apply:

- All HIPAA Privacy Group members should be assigned a unique identifier in order to be able to trace the individual's activity. The identifier should be of sufficient length and content, and changed periodically, in order to provide adequate security. Unique identifiers should not be changed unless the change has been approved by the Privacy Officer, and the new unique identifier has been logged.
- Access by HIPAA Privacy Group members to Protected Health Information on Company information systems shall be subject to all of the safeguards that generally apply, such as automatic shut-off, password protocols, hardware, software, and/or procedural mechanisms that record and examine activity on such systems.

4. GENERAL POLICIES

4.1 INTERPRETATION AND APPLICATION OF THE PRIVACY POLICY

The Privacy Officer, in consultation with the Security Officer where appropriate, shall have sole authority and discretion to resolve any questions or disputes concerning the interpretation or application of the provisions of the Privacy Policy, the HIPAA Privacy Rule, or the HIPAA Security Rule, subject to applicable requirements of law.

4.2 AMENDING THE PRIVACY POLICY

POLICY

The Privacy Officer, in consultation with the Security Officer where appropriate, has the right to make material changes to the Privacy Policy and to apply those changes to all Protected Health Information maintained by the Plan. When a material change is made in the Privacy Policy, such change shall conform to the requirements of the HIPAA Privacy Rule and the HIPAA Security Rule, and a corresponding change shall be made to the Notice of Privacy Practices. No material change in the Privacy Policy shall be implemented until an updated Notice of Privacy Practices incorporating the change(s) has been distributed to all individuals then covered under the Plan. The revisions to the Privacy Policy shall become effective on the effective date as set forth in the new Notice of Privacy Practices.

The Privacy Officer shall conform the Plan's Training Policy to the changes in the Privacy Policy.

4.3 MITIGATION OF KNOWN VIOLATIONS OF THE PRIVACY POLICY

POLICY

The Privacy Officer or the Security Officer, as applicable, shall mitigate, to the extent possible, any harmful effect of a use or disclosure of Protected Health Information that is known to the Privacy Officer or any member of the HIPAA Privacy Group to be in violation of the Privacy Policy, the HIPAA Privacy Rule, or the HIPAA Security Rule.

4.4 RECORD RETENTION AND DOCUMENTATION POLICY

POLICY

The Plan shall maintain the Privacy Policy and any changes thereto in written or electronic form. The Plan shall maintain a copy, in written form or electronically, of any communication required under the Privacy Policy, the HIPAA Privacy Rule, or the HIPAA Privacy Rule. Similarly, the Plan shall keep a written or electronic record of any action, activity or designation that is required to be documented under the HIPAA Privacy Rule or the HIPAA Privacy Rule. The Plan shall develop a system to maintain such documentation required by the HIPAA Privacy Rule for the longer of six years from the date of its creation or six years from the date when it was last in effect.

PROCEDURE

1. The following actions involving the use and disclosure of Protected Health Information, as well as any other instances specified in the HIPAA Privacy Rule or the HIPAA Privacy Rule, shall be documented by the appropriate member of the HIPAA Privacy Group:
 - Satisfactory assurances of Business Associates.
 - Authorizations.
 - Support for a disclosure with respect to a judicial or administrative procedure.
 - As necessary under the Verification Policy.
 - Providing the Notice of Privacy Practices.
 - Implementation of restrictions on Protected Health Information.
 - Subjecting a Designated Record Set to access.
 - Designations in general, including designations of persons to handle requests for restrictions, accounting and access to Protected Health Information.
 - Agency or official's oral statement requiring temporary suspension of individual's right to account for Protected Health Information.
 - Disclosures under the Privacy Policy as required under the Documenting Disclosures and Accounting Policy.
 - Training efforts of the Plan.
 - All complaints and the dispositions of the complaints.
 - Sanctions applied for violations.
 - Changes made to the Privacy Policy.
 - Designation of an affiliated entity.
2. Any correspondence that is received by a workforce member of the Company other than a member of HIPAA Privacy Group shall immediately be dated with the date of the receipt and forwarded to the HIPAA Privacy Group, without retaining a copy of such correspondence.

3. Such documentation shall be maintained in secured file cabinets dedicated solely to maintaining records and documentation under the HIPAA Privacy Rule. No other files, records or documentation of any kind shall be commingled with Protected Health Information, or the records required to be documented and maintained under the HIPAA Privacy Rule. Only members of the HIPAA Privacy Group shall have access to such cabinets.
4. In the event Protected Health Information or documentation is stored electronically, only members of the HIPAA Privacy Group shall have access to such files. The Privacy Officer shall cause to be put in place reasonable technological safeguards, such as establishing passwords or adjustments to network access or other means, to secure such files.
5. In the event an individual is no longer a member of the HIPAA Privacy Group, such person shall be required to surrender any key or other means of access to the documentation or Protected Health Information maintained by the Plan (e.g., keys to file cabinets). In addition, all means of access to electronic files shall be eliminated with respect to such person, such as changing the passwords granting access to such information.
6. From time to time, the Privacy Officer shall review the documentation and Protected Health Information maintained by the Plan and destroy any such materials no longer required to be maintained under the Privacy Policy.

4.5 REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

POLICY

The Company and the Plan shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising any of his or her rights under the HIPAA Privacy Rule. In addition, the Company and the Plan shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person for:

- filing a complaint with the Secretary of HHS;
- testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under HIPAA's "administrative simplification" provisions set forth at 42 USC 1302(d), et seq.; or
- opposing any act or practice that is unlawful under HIPAA Privacy Rule, provided the individual has a good faith belief that the practice to which he/she is opposed is indeed unlawful, and that the manner in which he/she voices his/her opposition is reasonable, and does not itself involve a disclosure of Protected Health Information that would violate the HIPAA Privacy Rule.

PROCEDURE

1. The Privacy Officer shall, when appropriate, as part of a workforce member's training, notify such workforce member that he or she may not retaliate against any individual for exercising any right such individual holds under the HIPAA Privacy Rule, and that if such workforce member becomes aware of, in any manner, a retaliatory act taken by any workforce member of the Company, such workforce member shall immediately notify the Privacy Officer.
2. The Privacy Officer shall follow the procedure for sanctioning the employee(s) responsible for the retaliatory or intimidating act.

4.6 SANCTIONS

POLICY

The Plan, through the Company, shall apply appropriate sanctions against any employee or other member of its workforce who knows or has reason to know that his or her actions or omissions would cause the Plan or the Company to fail to comply the Privacy Policy or any other federal or state mandated security or privacy rules.

Such sanctions shall NOT apply in the event of:

- A disclosure by a member of the Company's workforce or a Business Associate of the Company, provided: (i) the workforce member or Business Associate believes in good faith that the Company or the Plan, or a person acting on behalf of either the Company or the Plan, has engaged in conduct that is unlawful; and (ii) the disclosure is to a health oversight agency or public health authority authorized to oversee the relevant conduct, or to an attorney retained by or on behalf of the workforce member or Business Associate for the purpose of determining the legal options with respect to such conduct.
- A disclosure of Protected Health Information by a workforce member of the Company who is a victim of a criminal act to a law enforcement official, provided that: (i) the Protected Health Information is about the suspected perpetrator of the criminal act; and (ii) the Protected Health Information disclosed includes ONLY
 - name and address;
 - date and place of birth;
 - Social Security number;
 - ABO blood type and rh factor;
 - type of injury;
 - date and time of treatment;
 - date and time of death; and
 - distinguishing characteristics such as height, weight, gender, race, hair, eye color, presence or absence of facial hair, scars and tattoos.

Sanctions also shall NOT apply to any individual who:

- Files a complaint with the Secretary of HHS.
- Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing under HIPAA's "administrative simplification" provisions set forth at 42 USC 1302(d), et seq.
- Opposes any act or practice that is unlawful under the HIPAA security regulations or the HIPAA Privacy Rule, provided the individual has a good faith belief that the practice to which he/she is opposed is indeed unlawful, and that the manner in which he/she voices his/her opposition is reasonable, and does not itself involve a disclosure of Protected Health Information that would violate the HIPAA security regulations or the HIPAA Privacy Rule.

4.7 TRAINING POLICY

POLICY

The Privacy Officer and Security Officer shall collaborate to provide training to workforce members, including all members of the HIPAA Privacy Group, regarding the requirements of the Privacy Policy, the HIPAA Privacy Rule and the HIPAA Security Rule to the extent the Officers determine it is necessary and appropriate for such member to carry out his or her assigned task(s), including Security Incident response. Following the initial training, additional training shall be provided, as necessary and appropriate within the Officers' determination, for the purpose of reminding some or all of the members about certain aspects of the HIPAA Privacy Rule, HIPAA Security Rule, and the Privacy Policy, and to train such individuals with respect any changes in such policies.

5. GLOSSARY

The defined terms in this Glossary are intended to provide general information for the purpose of implementing the Privacy Policy. These terms, as well as all terms used in the Privacy Policy shall have the meaning ascribed to them in the HIPAA Privacy Rule and the HIPAA Security Rule, unless the context dictates otherwise.

Breach

means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under Subpart E of the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, as defined in 45 CFR 164.402.

Company

means Reliance Steel & Aluminum Co.

Designated Record Set

means a group of records maintained by or for the Plan that is

- the enrollment, payment, claims adjudication, and case or medical management records; or
- used, in whole or in part, by or for the Plan 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 Plan.

Health Information

means any information with respect to an individual covered under the Plan, whether oral or recorded in any form or medium, that

- is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future Payment for the provision of health care to an individual.

Individually Identifiable Health Information

is Health Information, including demographic information collected from an individual, and

- is created or received by the Plan;
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future Payment for the provision of health care to an individual; and
- that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Plan Administration Functions

means certain administration functions performed by the Company on behalf of the Plan and excludes functions performed by the Company in connection with any other benefit or benefit plan.

Protected Health Information

means Individually Identifiable Health Information:

1. Except as provided in paragraph (2) of this definition, that is
 - transmitted by electronic media;
 - maintained in any medium described in the definition of electronic media at § 162.103 of the HIPAA Privacy Rule; or
 - transmitted or maintained in any other form or medium.
2. Protected Health Information excludes Individually Identifiable Health Information in
 - education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
 - records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
 - employment records held by the Company in its role as employer. Thus, health information obtained by the Company in its capacity as an employer, such as in connection with the Family and Medical Leave Act, Americans with Disabilities Act, workers' compensation laws, is not protected under HIPAA.

Psychotherapy Notes

means 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 and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Security Incident

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

Summary Health Information

means information, that may be Individually Identifiable Health Information, and

- that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom the Company has provided health benefits under the Plan; and
- from which the information described at § 164.514(b)(2)(i) of the HIPAA Privacy Rule has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) of the HIPAA Privacy Rule need only be aggregated to the level of a five digit zip code.

Transaction

means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- Health care claims or equivalent encounter information.
- Health care payment and remittance advice.
- Coordination of benefits.
- Health care claim status.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health plan premium payments.
- Referral certification and authorization.
- First report of injury.
- Health claims attachments.
- Other transactions that the Secretary may prescribe by regulation.

Treatment

means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Unsecured Protected Health Information

means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS Web site.

6. APPENDIX

6.1 PLANS COVERED BY THE PRIVACY POLICY

The following group health plan benefits sponsored by Reliance Steel & Aluminum Co. are covered by the Privacy Policy:

- PPO Medical (Anthem Blue Cross)
- Prescription Drugs (CVS/Caremark)
- Dental (Delta Dental)
- Vision (Vision Service Plan)
- Health Care Flexible Spending Account (Aetna PayFlex)
- Employee Assistance Program (Anthem)

6.2 PRIVACY OFFICER, SECURITY OFFICER AND HIPAA PRIVACY GROUP DESIGNATIONS

Privacy Officer

Name: Vice President, Health, Safety and Human Resources shall serve as Privacy Officer.

Reports to: The Privacy Officer shall report to the **Chief Financial Officer**.

Security Officer

Name: Corporate Human Resources **Manager** shall serve as Security Officer.

Reports to: The Security Officer shall report to the Vice-President, Health, Safety, and Human Resources.

HIPAA Privacy Group

The following persons are members of the HIPAA Privacy Group as referred to in the Overview of Policies and Procedures to Protect the Privacy of Protected Health Information section of the Privacy Policy:

For all purposes under the Privacy Policy:

- Privacy Officer: Vice President, Health, Safety and Human Resources
- Security Officer: Corporate Human Resources Manager
- General Counsel
- HR Director, HR Manager, HR Generalist

For purposes of carrying out assigned tasks in the Finance/Accounting Department, including the processing of claims payments, working with external auditors and other purposes as determined by the Privacy Officer:

- Chief Financial Officer, Controller

For purposes of carrying out assigned tasks in the Information Technology Department, including information systems management and maintenance and other purposes as determined by the Privacy Officer:

- Director, Information Security, Security Analyst

For purposes of assessing compliance with internal policies and procedures in connection with reviewing employee files:

- HR Director, HR Manager, HR Generalist

6.3 SPECIFIC RULES FOR ACCESS AND USE OF PROTECTED HEALTH INFORMATION

Only HIPAA Privacy Group members are permitted to handle Protected Health Information. All HIPAA Privacy Group members shall ensure that any employees working under their supervision have a general understanding of the Privacy Policy's requirements. Such employees should be instructed to immediately forward to the HIPAA Privacy Group and retain no copies of any information likely to be Protected Health Information.

Mail/Telephone/Facsimile/Email Policies. The following procedures apply to the transfer of Protected Health Information via either regular mail, private courier, or other similar means; telephonically; and email or other electronic means:

- HIPAA Privacy Group members shall direct their respective employees who receive mail that may relate to or be Protected Health Information to forward that information directly to a HIPAA Privacy Group member.
- For incoming calls or emails requesting help furthering a claim under the Plan, all non-HIPAA Privacy Group members receiving such a call must immediately inform the requesting individual that he or she is not permitted to respond to questions regarding Plan benefit information and to direct the individual to contact the appropriate carrier, service provider or HIPAA Privacy Group member.
- All incoming mail that is reasonably likely to include Protected Health Information and is not addressed to any person's attention shall not be opened and shall be immediately forwarded to the Company's Human Resources Department. In the event the addressee is unreadable, the mailroom administrator shall forward that article to the Privacy Officer.
- All mail that is marked with "Personal and Confidential" or similar designations and addressed to an individual shall be forwarded to that individual unopened.
- All outgoing mail, including inter-office mail, containing Protected Health Information shall be sealed before it is processed.
- HIPAA Privacy Group members shall take reasonable steps to ensure that all incoming facsimiles and print jobs containing Protected Health Information are viewable and retrievable only by such members with a legitimate need for access. In addition, HIPAA Privacy Group members who transmit a facsimile must take reasonable steps to verify that the intended recipient is a person to whom such member is required, permitted, or authorized to disclose Protected Health Information under the Privacy Policy.
- HIPAA Privacy Group members must not fax Protected Health Information regarding an individual's spouse or child to that individual, unless such member (i) receives a signed authorization from that spouse or child prior to the disclosure; (ii) otherwise complies with the requirements of the Disclosures to Personal Representatives, Individuals, Family Members and Friends section of the Privacy Policy, or (iii) such disclosure is otherwise permissible under the Privacy Policy.

File management. HIPAA Privacy Group members shall keep and maintain Protected Health Information in locked file cabinets to which only they have access. HIPAA Privacy Group members shall take reasonable steps to ensure that access to electronically transmitted Protected Health Information is password protected. Electronically-stored Protected Health Information, including such information

residing in electronic mail messages, electronic document files, databases, floppy disks and other computer files must be password-protected and accessible only as permitted by the Privacy Policy.

HIPAA Privacy Group members shall log on to the appropriate electronic systems that access e-PHI only when there is a need to do so for immediately pending work and shall log off from such systems when they are no longer working on the pending matter. All HIPAA Privacy Group members shall enable the automatic logoff feature of the information systems through which they access e-PHI to cause the members to disconnect the member's connection to e-PHI due to inactivity after a reasonable period of time, determined by the Security Officer.

These files referred to above, "PHI files," whether in hard copy or electronic, shall include only Protected Health Information. That is, these PHI files shall be kept in separate file cabinets, file cabinet drawers or network locations and shall not include employment records or information even if the record or information is health related, such as in the case of records related to FMLA certification, disability claims, doctor's notes for personal leave, etc.

All questions regarding whether a record or information is Protected Health Information shall be resolved by the Privacy Officer. In the event Protected Health Information is not centrally located, each HIPAA Privacy Group member shall provide (and shall update as necessary) the Privacy Officer with (i) the location of all Protected Health Information and (ii) a copy of the key, the password or any other device or means necessary to access the Protected Health Information.

A designated member of the HIPAA Privacy Group shall maintain a log to document all repairs and modifications to the facility, including those repairs and modification that affect access to Protected Health Information, such as offices, file cabinets, file cabinet drawers, network locations, etc. The log shall include date and the reason for the repair. The Privacy Officer and/or Security Officer shall periodically review the log for the purpose of determining if there is a need to implement changes to a security policy and/or procedure based upon the recorded repairs and modifications.

If a HIPAA Privacy Group member needs to remove a laptop, floppy disk, CD or other transportable electronic device containing Protected Health Information from the office premises, he or she shall maintain such item or equipment in a secure location, and use all necessary steps to maintain the confidentiality of the information pursuant to the Privacy Policy.

7. FORMS AND NOTICES

7.1 FAQ'S TO EMPLOYEES REGARDING DATA PRIVACY AND SECURITY SAFEGUARDS

M e m o r a n d u m

TO: All Workforce Members/Employees

FROM: [INSERT NAME]

DATE:

RE: FAQs Re [PRACTICE]'S DATA PRIVACY AND SECURITY SAFEGUARDS

The Company's business needs require that it create, collect, use, process, modify, distribute, and, as appropriate, destroy records that contain confidential and personal information. This includes protected health information ("PHI") of participants in the group health plans ("Plans") the Company sponsors for employees and their families. In order to protect PHI, the Company maintains a comprehensive set of privacy and security policies and procedures ("Privacy Policy") to comply with HIPAA and other federal and state law mandates. This memo is intended to help you understand the key features of the Privacy Policy.

All members of the Company's workforce are subject to the Privacy Policy which applies to any and all PHI received, maintained, used or disclosed by the Company. Any questions concerning the Program should be directed to the Privacy Officer, or his or her designee.

1. What is Protected Health Information (PHI)?

In general, Protected Health Information is individually identifiable health information that relates to the Plans – the Company's group health plans sponsored for employees. Individually identifiable health information means information created or received by the Plans or the Company that relate to an individual's past, present or future (i) physical or mental health or condition, (ii) provision of health care, or (iii) payment for health care. The information could be "identifiable" even if the name is not included, but the information reasonably could identify the individual. Note that PHI does not just include identifiable information about an individual medical condition or diagnosis. A Plan member's name and Social Security Number in an EOB concerning the Plan with only billing codes is PHI.

Examples include: individual explanations of benefits (EOB), annual claim history, claim and appeals files and related information.

2. What is NOT Protected Health Information?

Not all medical information about an individual is subject to HIPAA. Medical information about employees collected or maintained by the Company in its capacity as an employer, without regard to the Plans, for example, is not PHI.

Examples include: FMLA, ADA, sick leave requests; disability insurance eligibility; drug screening results; workplace medical surveillance, fitness-for-duty testing.

3. Am I permitted to access PHI and how may I handle it?

Most Company employees are NOT permitted to access PHI. A designated set of employees have been given authority to access PHI, but only for plan administration purposes such as reviewing claims issues or for making changes to the Plans. Employees permitted to access PHI should only be doing so as necessary and appropriate to perform his or her job functions, and in accordance with the Privacy Policy adopted by the Company. For example, employees with access to PHI are not permitted to share it with employees who do not have access, unless the information relates to that employee or there is another permissible exception. If you have any questions about what information you are permitted to access, discuss with your direct supervisor or the Privacy Officer.

4. What kinds of steps should I be taking to safeguard PHI?

Again, unless you have been authorized to access PHI, you should not access or be in possession of PHI. However, whether authorized or not, if any member of the Company's workforce comes into possession of PHI, he or she should take steps to safeguard it and not disclose it further except as permitted under the Privacy Policy. In general, be sensible:

- For hard copy PHI
 - Limit the number of photocopies made of PHI.
 - Keep your desk clean. Put PHI away throughout the day and in closed and locked drawers or cabinets before leaving the office.
 - Follow the Company's data destruction procedure when PHI in paper format is obsolete or is not required to be retained for storage purposes.
 - Do not leave PHI unattended or in an unlocked conference room, cabinet or other container.
 - Do not leave PHI on a fax machine.
- For electronic PHI:
 - Destroy electronic PHI that is no longer needed, including cutting or destroying CDs or diskettes so that they are not readable.
 - Limit the use of PHI in e-mails, to the extent practical – follow the Minimum Necessary Rule to accomplish the intended purpose (e.g., refrain from forwarding strings of e-mail messages containing PHI).
 - Encrypt e-mail information as needed.

- Enable your screensaver to lock your computer automatically after 5 minutes of nonuse.
- Other safeguards:
 - When speaking to family members or friends of Plan participants, be sure they are authorized to be receiving that information. For example, if a spouse of an employee calls us to ask about an employee's denied claim under a Plan, you may not address the request until you have confirmed that the employee has authorized you to speak with the spouse about the issue.
 - Do not have conversations concerning PHI in places where other persons can overhear your discussion.
 - Request/access only the PHI you need to complete the task at hand.
 - Double check address information before sending mail or email containing PHI.
 - Do not take documents, laptops or flash drives or other items containing PHI out of the office, but if you have to in order to do your job, don't leave them in your car or on the train.
 - Do not access Company information systems or email through a unsecured wireless network, such as using the WiFi access available while traveling which may not be encrypted, and if you are in doubt as to the security of the network, do not use it.
 - If you have to disclose PHI, verify the person receiving it is authorized and disclose only what is minimally necessary for the intended purpose.

5. Can I disclose PHI to vendors or third parties?

First, you should only be accessing PHI if you have been designed by the Company to have access to PHI and authority to make disclosures. Before any vendor may access or receive PHI of the Plan, such as a claims administrator, benefits broker or law firm, the employee must work with the Privacy Officer (i) to assess the ability of the vendor to provide adequate safeguards to protect the PHI and (ii) ensure there is a Business Associate Agreement in place requiring the vendor to safeguard the PHI.

6. How is PHI handled in the claims and appeals process?

From time to time, it is necessary for the Company to become involved in the claim appeal process. The Company delegated the responsibility for this to the Benefits Appeals Committee which handles final appeals in accordance with Plan terms and the Privacy Policy. The steps it takes includes collecting information relevant to benefit determination, review and analysis of the claim, corresponding with Plan participant concerning the status of the determination and communicating with Business Associates as appropriate. For this reason, the Benefits Appeals Committee is permitted to access, use and disclosed PHI to the participant who is the subject of the appeal, health care providers involved with treating the participant, Business Associates involved in the claim and appeal determination process, and

other individuals and entities as permitted under the Privacy Policy. The PHI accessed, used and possibly disclosed for this purpose include copies of denial letters, documents submitted by the claimant, health care providers, etc., benefit determinations of participants' receiving similar services. PHI paper records will be maintained in the HR file room and clearly labeled —Health Plan Appeals. Electronic records will be retained on the HR shared folder. (Corporate Offices only). No redundant copies will be retained and PHI concerning claims will be destroyed 7 years after final resolution of the claim.

7. Can HR Staff continue to assist with eligibility and claims questions?

In general, those HR staff that have been permitted to access PHI, whether at the Company or any subsidiary or division, may assist Participants with various eligibility and claims questions consistent with the Privacy Policy and department guidelines. For example, HR Staff must remember to apply the Minimum Necessary Rule when accessing and disclosing PHI. If HR Staff have questions about the scope of requested disclosures, they should contact the Privacy Officer. HR Staff should store PHI paper records in the HR file room and clearly labeled —Customer Service - HIPAA. Electronic PHI must be retained on the HR shared folder (Corporate Offices only).

8. What happens if I learn of a breach - lose a laptop, send an email to the wrong person - where an unauthorized person gets access to or acquires PHI?

In the event you learn of an unauthorized access to or acquisition of PHI you must immediately report it to the Privacy Officer.

9. How do we handle requests for access to files that contain PHI?

We do not anticipate getting many requests for access to PHI, however, if we do we have to be careful when responding. For example, we generally need to verify the identity of the person making the request and his or her authority to be making the request. We also have to confirm we have the authority to make the disclosure.

Under HIPAA, the general rule is that PHI may not be disclosed without the authorization of the individual. This includes disclosing to the individual's spouse or in response to an attorney letter or subpoena. There are, of course, exceptions. For exception, if we receive a request from a vendor for the Plan relating to the vendors services and if there is a Business Associate Agreement in place, we can share PHI with the vendor without an authorization. However, if we receive a letter from an attorney for a former employee seeking "all of the employee's medical records of any kind," that request could include PHI we maintain for that employee with respect to the Plan. In that case, the disclosure generally should not be made without the former employee's authorization.

Also, even assuming a disclosure is permissible, whether pursuant to an authorization or now, we should only disclose the information that is responsive to the request, and nothing more.

10. How do we handle requests for amendments to PHI or accounting for disclosures of PHI?

We do not anticipate getting many requests for amending PHI or account for PHI disclosures, however, if we do we have to be careful when responding. First, only employees with access to PHI should be responding to these requests. If you do not have authority to access PHI and

receive such a request, please forward it to the Privacy Officer. Second, Section 2 of our Privacy Policy has detailed procedures and timeframe requirements for responding.

11. Will we be receiving training on this?

Many if not all employees have already received some training concerning data privacy and security of personal information. However, the Company plans on rolling out additional training on these topics, and employees with responsibilities concerning PHI will receive specific training in that area. However, if you have any questions in the meantime, please contact the Privacy Officer.

12. Can I be disciplined for failing to comply?

Just as with any other Company policy, failing to comply may subject you to discipline, up to and including termination.

7.2 AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION (GENERAL)

**RELIANCE STEEL & ALUMINUM CO.
AUTHORIZATION**

I, _____, or my personal representative designated below, hereby authorizes the use or disclosure of my health information as described in this Authorization.

The following items MUST be completed by the individual or his/her personal representative:

1. Name (or class) of person(s)/organization(s) authorized to disclose my health information:

2. Name (or class) of person(s)/organization(s) authorized to receive and use my health information:

3. Provide a specific and meaningful description of the health information you authorize to be disclosed (*Example*: “medical examination report and conclusions related to a fitness-for-work exam” or “results of drug testing for employment”):

4. State the purpose of the request (If you do not wish to state a purpose, please state, “at the request of the individual or personal representative.”):

The following paragraphs describe your rights with respect to this Authorization:

- I understand that I have the right to revoke this Authorization at any time by notifying in writing the person/organization authorized herein at **[Insert address]**. I understand that the

revocation is only effective after it is received and logged by such person/organization. I understand that any use or disclosure made prior to the revocation of this Authorization will not be affected by the revocation nor will the revocation apply to disclosures made in reliance on this Authorization.

- I understand that after the information is disclosed, federal or state law might not protect it and the recipient might redisclose it.
- I understand that my initial and continued employment and position are subject to my agreement to this Authorization, and any additional authorization Reliance Steel & Aluminum Co. requests.
- I understand that I am entitled to receive a copy of this Authorization.
- I understand this Authorization will expire (*please check one*)
 - ☐ when my employment with Reliance Steel & Aluminum Co. terminates.
 - ☐ once the purpose for this Authorization has been accomplished.
 - ☐ on _____ (*insert date*) or sooner in the event I revoke this Authorization in writing as provided above.
 - ☐ Upon (*describe event*): _____

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____
Date _____

**7.3 AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION
(PARTICIPANT ASSISTANCE)**

**RELIANCE STEEL & ALUMINUM Co.
AUTHORIZATION**

I, _____, or my personal representative designated below, hereby authorize human resources personnel of Reliance Steel & Aluminum Co. designated in the applicable employee benefit plan documents to use or disclose health information (then in their possession or provided by me) to the respective insurance carrier or third party provider for the purpose of assisting me with questions I have regarding benefit claims and other tasks related to furthering a claim for benefits I make under the applicable plan.

The following paragraphs describe your rights with respect to this Authorization:

I understand that I have the right to revoke this authorization at any time by notifying in writing the person/organization authorized herein at **[Insert address]**. I understand that the revocation is only effective after it is received and logged by such person/organization. I understand that any use or disclosure made prior to the revocation of the authorization will not be affected by the revocation nor will the revocation apply to disclosures made in reliance on this authorization.

I understand that after this information is disclosed, federal or state law might not protect it and the recipient might redisclose it.

I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits.

I understand that I am entitled to receive a copy of this authorization.

I understand this authorization will terminate with respect to each of the employee benefit plans under which I am covered when such coverage terminates, respectively.

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____
Date _____

**7.4 AUTHORIZATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION
(PARTICIPANT ASSISTANCE – SPOUSAL APPOINTMENT)**

**RELIANCE STEEL & ALUMINUM Co.
AUTHORIZATION**

I, _____, or my personal representative designated below, hereby authorizes the human resources personnel of Reliance Steel & Aluminum Co., acting on behalf of the Plan and designated in the applicable plan documents (HR Staff), to use or disclose my health information (in their possession or provided by me, my spouse named below or the Plan) to the respective insurance carrier or third party administrator for the purpose of assisting me with questions I have regarding benefit claims or otherwise related to furthering a claim for benefits available to me under the applicable plan. I also authorize the HR Staff to discuss the issues described above with my spouse _____.

By signing below, I acknowledge the following:

- I understand that I have the right to revoke this Authorization at any time by notifying in writing the person/organization authorized herein at **[Insert address]**. I understand that the revocation is only effective after it is received and logged by such person/organization. I understand that any use or disclosure made prior to the revocation of this Authorization will not be affected by the revocation nor will the revocation apply to disclosures made in reliance on this Authorization.
- I understand that after the information is disclosed, federal or state law might not protect it and the recipient might redisclose it.
- I understand that I may refuse to sign this Authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits.
- I understand that I am entitled to receive a copy of this Authorization.
- I understand this Authorization will terminate with respect to each of the employee benefit plans under which I am covered when such coverage terminates, respectively.

Signature of Individual _____

Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____

Date _____

7.5 BUSINESS ASSOCIATE AGREEMENT

RELIANCE STEEL & ALUMINUM CO. BUSINESS ASSOCIATE AGREEMENT

Effective _____, 20__

This BUSINESS ASSOCIATE AGREEMENT (the “Agreement”) is entered into by and among all group health plans sponsored by **[Insert Plan sponsor/employer name]** (referred to collectively as “Covered Entity”), **[Insert Plan sponsor/employer name]** (“Plan Sponsor”) and **[Insert company name]** (“Business Associate”).

I. DEFINITIONS

Except as otherwise provided herein, the terms used in this Agreement shall have the same meaning as those terms in the Electronic Transaction, Security or Privacy Rule, as the case may be.

Specific definitions:

(a) *Electronic Transaction Rule* means the standards for processing Standard Transactions and Code Sets at 45 CFR Parts 160 and 162.

(b) *Individual* has the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

(c) *Personal Information (“PI”)* means any data in whatever format that is subject to federal or state laws requiring the safeguarding of, and regulating and restricting access, collection, use, disclosure, processing, destruction, and free movement of individually identifiable personal information.

(d) *Privacy Rule* means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160-164.

(e) *Protected Health Information (“PHI”)* has the same meaning as the term “protected health information” in 45 CFR §160.103, including electronic protected health information, but limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(f) *Secretary* means the Secretary of the Department of Health and Human Services or his designee.

(g) *Security Rule* means the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160-164.

(h) *Final Rule* means the regulations issued by the Secretary which were published on January 25, 2013, that amend the Privacy Rule and Security Rule and implement the changes made under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as required by law. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule (specifically, Subpart E of 45 CFR Part 164), Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

(b) Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this Agreement. In addition, Business Associate agrees to implement administrative, physical and technical safeguards consistent with the requirements of the Security Rule that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate will comply with the Privacy Rule and the Security Rule to the extent required under Subpart C of 45 CFR Part 164 with respect to electronic PHI, and the Final Rule, which shall include but not be limited to 45 CFR Sections 164.308, 164.310, 164.312 and 164.316. Such safeguards shall be maintained pursuant to a written information security program which shall, at a minimum, include requirements for all of the following:

- designated individual responsible for safeguarding of PHI and PI;
- periodic risk assessments (no less frequently than annually) for appropriateness of safeguards and make appropriate modifications;
- information systems authentication and access controls;
- written incident response protocol and conduct annual incident response exercises as part of training;
- securing physical facilities, data centers, servers, back-up systems and computing equipment, including, but not limited to, encryption and password protection for all mobile devices and other equipment with information storage capability;
- disaster recovery and business continuity protocols; and
- securing all paper files, including without limitation redaction of PHI and PI where such information is not minimally necessary.

(c) Business Associate agrees to report to Covered Entity and/or Plan Sponsor (i) any use or disclosure of Protected Health Information not provided for by this Agreement, (ii) any Security Incident, (iii) any Breach of Unsecured Protected Health Information, or (iv) to the extent required under any state breach notification statute, any unauthorized acquisition or access to Personal Information, as soon as possible, but not later than 10 calendar days following the date it becomes aware of such use or disclosure, Security Incident, Breach or unauthorized acquisition or access.

(d) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information or Personal Information received from, or created or received by Business Associate on behalf of, Covered Entity, or who itself creates, receives, maintains or transmits Protected Health Information or Personal Information on behalf of Business Associate agrees in writing to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(e) Business Associate agrees to provide access, at the request of Covered Entity and in a reasonable time and manner, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to enable Covered Entity to meet the requirements under 45 CFR §164.524.

(f) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the request of Covered Entity or an Individual, and in a reasonable the time and manner as required under the Privacy Rule.

(g) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to. Covered Entity or the Secretary, in a reasonable time and manner or as designated by the Secretary, for purposes of determining Covered Entity's compliance with the Privacy Rule.

(h) Business Associate agrees to document all disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR §164.528. Business Associate further agrees to maintain and make available to Covered Entity all such documentation and information.

(i) Business Associate agrees to provide to Covered Entity or an Individual, in a reasonable time and manner, information collected in accordance with the preceding paragraph (i), to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR §164.528.

(j) Business Associate agrees to mitigate to the extent practicable any harmful effect known to Business Associate of any Security Incident, Breach of Unsecured Protected Health Information, or unauthorized acquisition or access to Personal Information.

(k) If Business Associate conducts any Standard Transaction for or on behalf of Covered Entity, Business Associate shall comply with the requirements under the Electronic Transaction Rule.

(l) To the extent Business Associate creates or receives Personal Information from Covered Entity or Plan Sponsor, or on behalf Covered Entity or Plan Sponsor, it shall collect, maintain, process, handle, use, disclose and destroy all Personal Information in compliance with all applicable data privacy and protection laws (including without limitation the 20 controls set forth in the Center for Internet Security's Critical Security Controls and the Massachusetts data security regulations set forth at 201 CMR 17.00 et seq.) and maintain a comprehensive data privacy and security program, which shall include appropriate administrative, physical, technical and organizational measures to safeguard such data against the unauthorized access, possession, use, knowledge, process, disclosure, destruction, loss, alteration or theft, and which shall be no less rigorous than generally accepted privacy and security standards.

(m) To the extent any Breach of Unsecured Protected Health Information or unauthorized acquisition or access to Personal Information is attributable to a breach of the obligations under this Agreement by Business Associate, Business Associate shall bear the costs incurred by Covered Entity and Plan Sponsor to the extent it is necessary for Covered Entity and Plan Sponsor to comply with its legal obligations relating to such breach under the applicable breach notification statute or regulation, which shall include the following costs reasonably incurred by Covered Entity and Plan Sponsor in responding to such breach: (1) the reasonable cost of preparing and distributing notifications to affected individuals, (2) the reasonable cost of providing notice to government agencies, credit bureaus, and/or other required entities, (3) the reasonable cost of providing affected individuals with credit monitoring services for a specific period not to exceed twelve (12) months, or longer if required by law, (4) the reasonable cost of call center support for such affected individuals for a specific period not to exceed thirty (30) days from

the date the breach notification is sent to such affected individuals, and (5) the reasonable cost of any other measures required under applicable law.

(n) To the extent Business Associate receives, stores, processes or otherwise deals with any patient records from the Covered Entity or Plan Sponsor that are entitled to protection under the federal regulations issued at 42 CFR Part 2, Business Associate agrees to be bound by those regulations. In addition, if necessary, Business Associate will resist in judicial proceedings any efforts to obtain access to such patient records except as permitted by 42 CFR Part 2.

(o) Except for payments from Covered Entity for services performed pursuant to this Agreement and the Services Agreement, Business Associate may not directly or indirectly receive remuneration in exchange for PHI or PI.

(p) Business Associate may not use or disclose Protected Health Information or Personal Information for research or marketing purposes without first receiving prior written approval from the Covered Entity and obtaining the necessary authorization from the affected individuals.

(q) Business Associate agrees to implement an Identity Theft Monitoring Policy and Procedure, consistent with the requirements of the “Red Flags” rule adopted by the Federal Trade Commission, as applicable.

(r) If the Business Associate conducts any standard transaction for, or on behalf of, a Covered Entity, the Business Associate shall comply, and shall require any subcontractor or agent conducting such standard transaction to comply, with each applicable requirement of Title 45, Part 162, of the Code of Federal Regulation. The Business Associate shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in connection with the conduct of standard transactions for, or on behalf of, Covered Entity that:

- Changes the definition, health information condition, or use of a health information element or segment in a standard;
- Adds any health information elements or segments to the maximum defined health information set;
- Uses any code or health information elements that are either marked “not used” in the standard’s implementation specification(s) or are not in the standard’s implementation specifications(s); or
- Changes the meaning or intent of the standard’s implementations specification(s).

III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the **[Insert name of underlying services agreement]** dated **[Insert date]** (“Services Agreement”), provided that such use or disclosure would not violate (i) the Privacy Rule if done by Covered Entity or (ii) the minimum necessary policies and procedures of the Covered Entity supplied to Business Associate.

Specific Use and Disclosure Provisions

(a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that (i) disclosures are required by law, or (ii)(A) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and (ii)(B) the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except to the extent prohibited by law, Business Associate shall immediately notify Covered Entity upon its receipt of a request for use or disclosure of Protected Health Information or Personal Information with which Business Associate believes it is required by law to comply. Business Associate shall provide Covered Entity with a copy of such request, shall consult and cooperate with Covered Entity concerning the proper response to such request and shall provide Covered Entity with a copy of any information disclosed pursuant to such request.

(d) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B).

(e) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

IV. OBLIGATIONS OF COVERED ENTITY

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

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

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

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Requests by Covered Entity

(a) Except as otherwise provided in this Agreement, Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

V. TERM AND TERMINATION

(a) *Term.* The term of this Agreement shall be effective as of the date specified above, and shall terminate when all of the Protected Health Information and Personal Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information as determined by Business Associate, protections are extended to such information, in accordance with the termination provisions in this Section, subject to any record retention requirements under the Agreement or required by law.

(b) *Termination for Cause.* Upon either party's knowledge of a material breach of the Agreement by the other party, the non-breaching party shall either:

(1) Provide an opportunity for breaching party to cure the breach or end the violation and terminate this Agreement and the underlying services agreement, if any, if the breaching party does not cure the breach or end the violation within a reasonable time specified by the non-breaching party; or

(2) Immediately terminate this Agreement and the underlying services agreement, if any, if the breaching party has breached a material term of this Agreement and, in the non-breaching party's sole discretion, cure is not possible.

(c) *Effect of Termination.*

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information and Personal Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information and Personal Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information and Personal Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information and Personal Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon such determination that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections and obligations of this Agreement to such Protected Health Information and Personal Information and limit further uses and disclosures of such Protected Health Information and Personal Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information and Personal Information.

VI. MISCELLANEOUS

(a) *Regulatory References.* A reference in this Agreement to a section in the Electronic Transaction, Privacy or Security Rule means the section as in effect or as amended.

(b) *Amendment.* In the event that additional standards are promulgated, or any existing standards are amended, including without limitation the Privacy Standards, Security Standards, and the Transactions and Code Sets Standards, the parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA, or any applicable state law, as amended. Except as herein otherwise provided, no amendment or

modification of, or supplement to, this Agreement shall be binding unless duly executed in writing by each of the parties hereto.

(c) *Survival.* The respective rights and obligations of Business Associate under the Section of this Agreement entitled "Effect of Termination" shall survive the termination of this Agreement.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Electronic Transaction, Privacy or Security Rule.

(e) *Cooperation.* Business Associate with fully cooperate with Covered Entity and render such assistance as may be reasonably required in the event of litigation or administrative proceedings with respect to any violation or claimed violation of the HIPAA Privacy and Security Standards, related laws, or state breach notification laws.

(f) *Right of Audit.* The Covered Entity shall have the right at all reasonable times and upon reasonable notice to Business Associate to audit and examine the policies, procedures, and records of the Business Associate insofar as such audit and examination directly relates to, and is limited by, the Business Associate's obligations as set forth under this Agreement. Such audits may involve examinations of a representative portion of uses and disclosures of the Protected Health Information, the safeguards implemented by the Business Associate to protect Protected Health Information or Personal Information, which could include access to Business Associate's facilities used for the maintenance and processing of Protected Health Information or Personal Information. The Covered Entity shall bear all reasonable expenses of the audit.

(g) *Indemnification.* Notwithstanding any provision of the Services Agreement to the contrary, in the event the Covered Entity or Plan Sponsor to this Agreement, or any of their officers, employees, or agents (collectively, the Indemnified Party) are made parties to any judicial or administrative proceeding or similar action relating to claims, investigations, complaints, or inquiries arising in whole or in part out of the alleged or actual negligent or unlawful performance by the Business Associate (collectively, the Indemnifying Party) or its employees, agents or subcontractors of any of the Indemnifying Party's obligations under this Agreement, the Indemnifying Party shall indemnify, defend and hold the Indemnified Party harmless for any and all judgments, settlements, damages and costs (including without limitation: reasonable attorneys' fees and civil penalties under the Privacy and Security Rules, or applicable state law) which the Indemnified Party incurs or pays in connection therewith.

(h) *Counterparts.* This Agreement may be executed in two or more counterparts, each of which together shall be deemed an original, but all of which together shall constitute one and the same instrument. In the event that any signature is delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of the party executing (or on whose behalf such signature is executed) with the same force and effect as if such facsimile or ".pdf" signature page were an original thereof.

(i) *Successors and Assigns.* This Agreement and each party's obligations hereunder will be binding on the representatives, assigns, and successors of such party and will inure to the benefit of the assigns and successors of such party; provided, however, that any such assignment shall not be effective absent the consent of the non-assigning party which shall not unreasonably withheld or delayed.

(j) *No Third Party Beneficiaries.* Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than parties and their respective successors or assigns, any rights, remedies or obligations whatsoever.

(k) *Nature of relationship.* No provision of this Agreement is intended to create, nor shall be deemed or construed to create, any employment, agency or joint venture relationship between the Covered Entity, the Plan, and Business Associate other than that of independent entities contracting with each other hereunder solely for the purpose of effectuating the provisions of this Agreement and the underlying agreements. None of the parties nor any of their respective representatives shall be construed to be the agent, employer, or representative of the other. The parties have reviewed the factors to determine whether an agency relationship exists under the federal common law of agency and it is not the intention of either the Covered Entity, the Plan, or Business Associate that Business Associate constitute an “agent” under such common law.

(l) *Governing Law.* This Agreement will be governed by and interpreted in accordance with the laws of the State of New Jersey, without regard to principles of conflicts of law. Each party irrevocably agrees that any legal action, suit or proceeding brought by it in any way arising out of this Agreement must be brought solely and exclusively in state or federal courts located in the State of New Jersey, and each party irrevocably submits to the sole and exclusive jurisdiction of these courts in personam, generally and unconditionally with respect to any action, suit or proceeding brought by it or against it by the other party.

(m) *Entire Agreement.* This Agreement sets forth the full and complete understanding of the parties hereto with regard to its subject matter. It replaces, supersedes and restates all prior agreements concerning its subject matter.

(n) *Waiver.* The failure of the Covered Entity or Business Associate to object or to take affirmative action with respect to any conduct of the other which is in violation of this Agreement shall not be construed as a waiver of that violation or any prior or future violations of this Agreement.

(o) *Headings.* The sections and subsections headings used herein are for reference and convenience only, and shall not enter into the interpretation thereof.

(p) *Notices.* Any notice which is to be given by one party to the other under this Agreement will be given in writing and delivered to the address of the other party set out below or any other address specified subsequently. A notice will be effective upon receipt thereof by the other party. Either party may change its address for service by giving notice to the other party in accordance with this paragraph.

If to Covered Entity:
[Insert address]

If to Business Associate:
[Insert address]

Attn: **[Insert name]**

Attn: **[Insert name]**

IN WITNESS WHEREOF, the parties have caused this Agreement to be signed by their duly authorized representatives or officers, effective as of the date specified above.

COVERED ENTITY:

BUSINESS ASSOCIATE:

By: _____
Name: _____
Title: _____
Date: _____

By: _____
Name: _____
Title: _____
Date: _____

PLAN SPONSOR:

By: _____

Name: _____

Title: _____

Date: _____

7.6 HIPAA PRIVACY CONFIDENTIALITY AGREEMENT

RELiance STEEL & ALUMINUM Co. HIPAA PRIVACY CONFIDENTIALITY AGREEMENT

Effective _____, 20__

I, _____, have read and agree to comply with Reliance Steel & Aluminum Co.'s Privacy Policy ("Privacy Policy") regarding the privacy of Individually Identifiable Health Information in what ever format, including electronic ("Protected Health Information").

I acknowledge that I have received training in such policies concerning Protected Health Information use, disclosure, storage and destruction.

In consideration of my employment or compensation from Reliance Steel & Aluminum Co., I hereby agree that:

- I will not at any time - either during my employment or association with Reliance Steel & Aluminum Co. or after my employment or association ends - use, access or disclose Protected Health Information to any person or entity, internally or externally, except (i) as is required and permitted in the course and scope of the duties of the position to which I have been assigned, (ii) as set forth in the Privacy Policy or (iii) as permitted under the HIPAA Privacy Rule.
- This obligation extends to any Protected Health Information that I may acquire during the course of my employment or association with Reliance Steel & Aluminum Co., whether in oral, written, electronic or any other form and regardless of the manner in which access was obtained.
- I will comply with the requirements of the Privacy Policy during the course of my employment or association.
- Unauthorized uses or disclosures of Protected Health Information may result in disciplinary action, up to and including the termination of my employment or association with Reliance Steel & Aluminum Co. Civil or criminal penalties under applicable federal and state law, as well as professional disciplinary action, may also apply.
- The terms of this agreement and my obligations hereunder shall survive the termination of my employment or end of my association with Reliance Steel & Aluminum Co., regardless of the reason for such termination.

Signed

Date

7.7 PROTECTED HEALTH INFORMATION DISCLOSURE LOG

**RELIANCE STEEL & ALUMINUM Co.
PROTECTED HEALTH INFORMATION DISCLOSURE LOG**

Individual's name: _____ Date of birth _____

Dates Covered by this Accounting Sheet: _____ to _____

The individual has the right to an accounting of disclosures made up to six (6) years prior to the date of the request

Date	Protected Health Information disclosed	To Whom Disclosed Name/Address	Basis for Disclosure	For multiple disclosures to single person/entity for single purpose, frequency, and date of last disclosure for accounting period.

7.8 BREACH NOTIFICATION FORM LETTER

[RELIANCE STEEL & ALUMINUM CO.] LETTERHEAD]

[Insert name]
[Insert address]

Dear [Insert name],

On [Insert date], a [Insert Company name and reason for notice. For example: “employee’s company laptop was stolen”]. We learned of the incident on [Insert date]. The [Identify what was lost/stolen that contained the personal information] contained certain personal information about [Identify about whom the personal information relates] including name, [Identify the types of personal information lost. For example, social security number, date of birth, etc.].

[Insert first sentence if applicable]Immediately upon discovering the theft, [Insert Company name] filed a report with the [Insert police department name] Police Department and an investigation is underway. We are not aware of any improper access or use of the personal information contained on the laptop. Nonetheless, we are sending this advisory to you and other individuals whose personal information may have been contained in the laptop to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. The attached sheet describes steps you can take to protect your identity, credit and personal information.

While we believe that there is little likelihood your information will be misused as a result of this incident, as a precaution we have arranged for [Insert name of third party provider] to provide you with [Insert Number of Months] months of credit monitoring and related services at no cost to you. **To receive these services you must enroll with [Insert name of third party provider] within 60 days of the date of this letter.**

Beginning [Insert date], a call center and toll-free number will be available to you for purposes of (i) enrolling in the program, (ii) assisting you in learning more about identity theft solutions, and (iii) answering some of your questions regarding the incident. To enroll, call [Insert name of third party provider] at [Insert telephone number]. The services include [Insert description of services]. In addition, if over the course of the next [Insert period], you believe your identity has been stolen and is being misused, contact [Insert name of third party provider] by calling [Insert telephone number], and a [Insert name of third party provider] representative will be available, at no cost to you, to help you correct the fraud.

We apologize for this situation and any inconvenience it may cause you.

We treat all sensitive employee information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring.

If you have questions or concerns you should call [Insert name of third party provider] at [Insert telephone number]. You can also contact me at [Insert telephone number/contact information].

Sincerely,

[Insert name and title]

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
P.O. Box 740256
Atlanta, GA 30374
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com/consumer

TransUnion
P.O. Box 2000
Chester, PA 19022
(800) 888-4213
www.transunion.com

2. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues and how to avoid identity theft. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

7.9 NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

RELIANCE STEEL & ALUMINUM CO. NOTICE OF PRIVACY PRACTICES

Effective as of **[Insert 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.

The privacy practices described in this notice apply to the group health plans sponsored by Reliance Steel & Aluminum Co.(referred to collectively as the “Plan”). The Plan is required by the federal law known as the Health Insurance Portability and Accountability Act (referred to as the HIPAA Privacy Rule) to make reasonable steps to ensure the privacy of your personally identifiable health information (*Protected Health Information*) and to inform you about:

- your Plan’s uses and disclosures of *Protected Health Information*;
- your privacy rights with respect to your *Protected Health Information*;
- your right to file a complaint with your Plan and to the Secretary of the U.S. Department of Health and Human Services; and
- the person or office to contact for further information about your Plan’s privacy practices.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Except as otherwise described in this notice or otherwise permitted under the HIPAA Privacy Rule, uses and disclosures of *Protected Health Information* will be made only with your written authorization subject to your right to revoke such authorization. If you provide the Plan authorization to use or disclose PHI about you, you may revoke that permission, in writing, at any time by sending a notice of revocation to the Privacy Officer at the address provided below. If you revoke your permission, the Plan will no longer use or disclose PHI about you for the reasons covered by your written authorization. The Plan will not be able to reverse any disclosures made prior to your revocation.

USES AND DISCLOSURES TO CARRY OUT TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

The HIPAA Privacy Rule permits the Plan and its respective Business Associates to use and disclose *Protected Health Information* without your consent, authorization, or opportunity to agree or object, to carry out Treatment, Payment and Health Care Operations.

- *Treatment* is the provision, coordination or management of health care and related services. For example, a Business Associate of the Plan may disclose to a treating orthodontist the name of your treating dentist so that the orthodontist may ask for your dental X-rays from the treating dentist.
- *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). For example, a Business Associate of the Plan may tell a doctor whether you are eligible for coverage or what percentage of the bill will be paid by the Plan.

- *Health Care Operations* include but are 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. For example, the Plan may use information about your claims to refer you to a disease management program, project future benefit costs or audit the accuracy of its claims processing functions.

In addition, your Plan may use or disclose enrollment information to the “Company” (Reliance Steel & Aluminum Co.) as well as “summary health information” for obtaining premium bids or modifying, amending or terminating the group health plan, which summarizes the claims history, claims expenses or type of claims experienced by individuals for whom an employee of the Company has enrolled in health benefits under a group health plan, and from which identifying information has been maintained in accordance with HIPAA. Your Plan may also disclose *Protected Health Information* to the Company for treatment, payment or health care operations and plan administration purposes as permitted under HIPAA, which includes disclosing such information to Business Associates of the Plan. Note also that your Plan may not use or disclose genetic information for underwriting purposes.

Note: Special rules may apply with respect to the use and disclosure of genetic and HIV testing information. You may contact the Privacy Officer for more information about these rules.

USES AND DISCLOSURES THAT REQUIRE YOUR WRITTEN AUTHORIZATION

Your written authorization is generally required before the Plan will use or disclose psychotherapy notes about you from your psychotherapist, as well as most disclosures of PHI for which the Plan receives remuneration or for marketing purposes. Psychotherapy notes are separately filed notes about your conversations with your mental health professional during a counseling session. They do not include summary information about your mental health treatment. The Plan may use and disclose such notes when needed by the Plan to defend against litigation filed by you.

To the extent your Plans uses and discloses your Protected Health Information for certain marketing purposes, it will obtain your specific authorization to the extent required by law. Additionally, any disclosures that constitute the sale of your Protected Health Information will also require your specific authorization.

USES AND DISCLOSURES THAT REQUIRE THAT YOU BE GIVEN AN OPPORTUNITY TO AGREE OR DISAGREE PRIOR TO THE USE OR RELEASE

Disclosure of your *Protected Health Information* to family members, other relatives and your close personal friends is allowed if:

- the information is directly relevant to the family or friend’s involvement with your care or payment for that care; and
- you have either agreed to the disclosure or have been given an opportunity to object and have not objected.

OTHER USES AND DISCLOSURES FOR WHICH CONSENT, AUTHORIZATION OR OPPORTUNITY TO OBJECT IS NOT REQUIRED

Use and disclosure of your *Protected Health Information* is allowed without your consent, authorization or request under the following circumstances:

- When required by law.

- When permitted for purposes of public health activities, including if you have been exposed to a communicable disease or are at risk of spreading a disease or condition, if authorized by law.
- When authorized by law to report information about certain abuse, neglect or domestic violence to public authorities.
- For public health oversight activities authorized by law.
- For certain judicial or administrative proceedings.
- For certain law enforcement purposes
- To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as authorized by law; and funeral directors, consistent with applicable law.
- The Plan may use or disclose *Protected Health Information* for research, subject to conditions.
- For the purpose of facilitating organ, eye or tissue donation or transplantation.
- When consistent with applicable law to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
- To the extent necessary to comply with workers' compensation or other similar programs established by law.

REQUIRED USES AND DISCLOSURES

Upon your request, your Plan is required to give you access to certain *Protected Health Information* in order to inspect and copy it. Under certain circumstances, however, the Plan may deny your request.

Use and disclosure of your *Protected Health Information* may be required by the Secretary of the Department of Health and Human Services to investigate or determine the Plan's compliance with the privacy regulations.

RIGHTS OF INDIVIDUALS

In the event any of the following rights require you to submit a written request to exercise such right, you must submit such request to the Privacy Officer, **[Insert address]**.

RIGHT TO REQUEST RESTRICTIONS AND CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION

You may request that your Plan restrict uses and disclosures of your *Protected Health Information* to carry out Treatment, Payment or Health Care Operations, or to restrict uses and disclosures to persons identified by you who are involved in your care or payment for your care. The Plan is not required to agree to your request.

Your Plan will accommodate reasonable requests to receive communications of *Protected Health Information* by alternative means or at alternative locations. You or your personal representative will be required to complete a form to request confidential communications of your *Protected Health Information*.

RIGHT TO INSPECT AND COPY PROTECTED HEALTH INFORMATION

You have a right to request to inspect and obtain a copy of your *Protected Health Information* contained in a "Designated Record Set," for as long as your Plan maintains the *Protected Health Information*.

- “Designated Record Set” includes enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a health plan, or other information used in whole or in part by or for the Covered Entity to make decisions about individuals. Information used for quality control or peer review analyses and not used to make decisions about individuals is not in the Designated Record Set.

The requested information will be provided within 30 days. A single 30-day extension is allowed if your Plan or its Business Associates are unable to comply with the deadline. Your Plan will charge a reasonable, cost-based fee to cover the cost of providing copies.

You or your personal representative will be required to complete a form to request access to the *Protected Health Information* in your Designated Record Set. 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 those review rights and a description of how you may complain to the Secretary of the U.S. Department of Health and Human Services.

RIGHT TO AMEND PROTECTED HEALTH INFORMATION

You have the right to request your Plan to amend your *Protected Health Information* or a record about you in a Designated Record Set for as long as the *Protected Health Information* is maintained in the Designated Record Set.

The Plan has 60 days after the request is made to act on the request. A single 30-day extension is allowed. If the request is denied in whole or part, your Plan must provide you with a written denial that explains the basis for the denial. 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 your *Protected Health Information*.

You or your personal representative will be required to complete a form to request amendment of the *Protected Health Information* in your Designated Record Set. Any request for an amendment must be in writing and provide a reason to support a requested amendment.

RIGHT TO RECEIVE AN ACCOUNTING OF PROTECTED HEALTH INFORMATION DISCLOSURES

Upon your written request, your Plan will also provide you with an accounting of disclosures by the Plan of your *Protected Health Information* during the six years prior to the date of your request. However, such accounting need not include *Protected Health Information* disclosures made: (1) to carry out Treatment, Payment or Health Care Operations; (2) to individuals about their own *Protected Health Information*; (3) prior to the compliance date; or (4) based on your written authorization.

If the accounting cannot be provided within 60 days, an additional 30 days is allowed if the individual is given 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, your Plan will charge a reasonable, cost-based fee for each subsequent accounting.

RIGHT TO NOTIFICATION OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION.

In the event that a breach occurs with regard to your unsecured Protected Health Information, you have the right to be notified of the breach.

A NOTE ABOUT PERSONAL REPRESENTATIVES

You may exercise your rights through a personal representative. Your personal representative will be required to produce evidence of his/her authority to act on your behalf before that person will be given access to your *Protected Health Information* or allowed to take any action for you.

Your Plan retains discretion to deny access to your *Protected Health Information* 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.

YOUR PLAN'S DUTIES

Your Plan is required by law to maintain the privacy of *Protected Health Information* and to provide participants and beneficiaries with notice of its legal duties and privacy practices. This notice is effective beginning **[Insert date]** and the Plan is required to comply with the terms of this notice. However, the Plan reserves the right to change its privacy practices and to apply the changes to any *Protected Health Information* received or maintained by the Plan prior to that date.

If a privacy practice is materially changed, a revised version of this notice will be provided to all participants then covered under the Plan. The revised notice in the preceding sentence shall be provided by first class mail to the individual's last known address. 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, the individual's rights, the duties of your Plan or other privacy practices stated in this notice.

MINIMUM NECESSARY STANDARD

When using or disclosing *Protected Health Information* or when requesting *Protected Health Information* from another Covered Entity, the Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of *Protected Health Information* 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 the individual or pursuant to your authorization;
- disclosures for compliance made to the Secretary of the U.S. Department of Health and Human Services;
- uses or disclosures that are required by law; and
- uses or disclosures that are required for the Plan's compliance with legal regulations.

YOUR RIGHT TO FILE A COMPLAINT WITH THE PLAN OR THE HHS SECRETARY

If you believe that your privacy rights have been violated, you may complain to your Plan in care of the following officer: Privacy Officer, **[Insert address]**, or you may call **[Insert telephone number]**.

You may file a complaint with the Secretary of the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, 200 Independence Avenue S.W., Washington, D.C. 20201. Your Plan will not retaliate against you for filing a complaint.

ADDITIONAL INFORMATION

If you have any questions regarding this notice or the subjects addressed in it, you may contact the following officer: Privacy Officer, **[Insert address]**, or you may call **[Insert telephone number]**.

The HIPAA Privacy Rule is set out at 45 Code of Federal Regulations Parts 160 and 164. These regulations and additional information about the HIPAA Privacy Rule are available at <http://www.hhs.gov/ocr/hipaa/>.

7.10 REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

RELIANCE STEEL & ALUMINUM CO. REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

I, _____, or my personal representative designated below, hereby request that the group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") permit me to access my health information described below and in the following manner:

This request relates to the following health information:

Please check one of the items below:

- ☐ I would like the Plan to permit me or my personal representative access to the health information described above for inspection.
- ☐ I would like the Plan to provide me or my personal representative with copies of the health information described above. ***By making this request, I agree to reimburse the Plan for any and all costs it incurs in providing the copies requested.***

I understand that under some circumstances the Plan is permitted to deny my request.

I understand that the Plan will generally respond to my request within 30 days after it receive this request. In addition, in the event the Plan is unable to respond with the timeframes mentioned above, I understand that the time for responding may be extended for one time for no longer than 30 days.

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____
Date _____

7.11 REQUEST TO AMEND PROTECTED HEALTH INFORMATION

RELIANCE STEEL & ALUMINUM CO. REQUEST TO AMEND PROTECTED HEALTH INFORMATION

I, _____, or my personal representative designated below, hereby request that the group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") amend the Protected Health Information in its Designated Record Set.

Specifically describe the amendment requested:

Specifically describe the reason for the amendment requested:

I understand that under some circumstances the Plan is permitted to deny my request. For example, I understand that the Plan is not required to honor my request if the Protected Health Information: (i) was not created by the Plan; (ii) is not part of the Designated Record Set; (iii) would not be available to me to access; or (iv) is accurate and complete.

I understand that the Plan will generally respond to my request within 60 days after it receives this request. If, however, the Plan is unable to respond with the timeframe mentioned above, I understand that the time for responding may be extended for one time for no longer than 30 days.

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____
Date _____

7.12 COMPLAINT FORM

RELIANCE STEEL & ALUMINUM CO.

COMPLAINT FORM

I, _____, or my personal representative designated below, hereby submit the following complaint to the group health plan sponsored by Reliance Steel & Aluminum Co. (“Plan”) regarding its Privacy Policy.

Specifically describe your complaint:

[illegible]

I attest under penalties of perjury that the above complaint is true and correct to the best of my knowledge.

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of:

Signature of Personal Representative _____
Date _____

7.13 REQUEST FOR CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION

**RELIANCE STEEL & ALUMINUM Co.
REQUEST FOR CONFIDENTIAL COMMUNICATIONS OF PROTECTED
HEALTH INFORMATION**

I, _____, or my personal representative designated below, hereby request that the group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") communicate Protected Health Information to me through the following alternative means and/or at the following alternative locations:

Specify the alternative means requested:

Specify the alternative locations:

I understand that the Plan may deny this request if the Privacy Officer finds it to be unreasonable or finds that the Plan cannot accommodate the request. I understand that I will be notified in the event the Plan cannot accommodate this request.

I understand that the Plan may not require me to explain the basis for this request. I understand that the disclosure of all or part of the information to which this request pertains could put me in danger.

Signature of Individual _____

Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____

Date _____

7.14 REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

RELIANCE STEEL & ALUMINUM CO. REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

I, _____, or my personal representative designated below, hereby request that the group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") provide an accounting of all the disclosures of my health information it has made for the period beginning on _____ and ending on _____.

I understand that this request may not relate to a disclosure of Protected Health Information made by the Plan more than 6 years before the date of this request.

Please check one of the items below:

- ☐ I understand that because this is my first request for an accounting of disclosures of my Protected Health Information in a 12-month period, the accounting shall be provided without charge.
- ☐ I understand that because I have already made one request for an accounting of disclosures of my Protected Health Information during this 12-month period, ***I agree to reimburse the Plan for any and all costs it incurs in providing the accounting requested.***

I understand that the Plan is not required to document certain disclosures and that as such those disclosures are not subject to this request. In addition, I understand that under certain circumstances my right to have an accounting of the disclosures of my Protected Health Information may be suspended by a health oversight committee or a law enforcement agency.

I understand that for disclosures the Plan must account for, the accounting shall provide:

- The date of the disclosure.
- The name and, if known, the address of the person to whom the disclosure was made.
- A brief description of the Protected Health Information which was disclosed.
- A brief statement of the purpose for the disclosure that reasonably sets forth the basis upon which the disclosure was made.

I understand that the Plan will generally respond to my request within 60 days after it receive this request. In addition, in the event the Plan is unable to respond with the timeframe mentioned above, I understand that the time for responding may be extended one time for no longer than 30 days.

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____

Date _____

7.15 REQUEST FOR A RESTRICTION ON PROTECTED HEALTH INFORMATION

RELIANCE STEEL & ALUMINUM CO. REQUEST FOR A RESTRICTION ON PROTECTED HEALTH INFORMATION

I, _____, or my personal representative designated below, hereby request that the group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") restrict access to my health information as described below:

Describe the Protected Health Information that is the subject of this request and the type of restrictions you would like placed on this information: (Attach a separate form if necessary.)

I understand that the Plan is not required to agree to the restriction requested above. In addition, I understand that if I am in need of emergency treatment and the information that is the subject of this request is needed to provide such treatment, the Plan may disclose the information to a provider in order to provide the treatment, regardless of the restriction described above.

Signature of Individual _____
Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this Authorization on the basis of: _____

Signature of Personal Representative _____
Date _____

7.16 RESPONSE TO INDIVIDUAL’S REQUEST TO ACCESS PROTECTED HEALTH INFORMATION

[RELIANCE STEEL & ALUMINUM CO.] **LETTERHEAD]**

[Insert date]

[Insert name of individual or personal representative]
[Insert address]

RE: Request to Access Protected Health Information

Dear **[Insert name of individual or personal representative]**:

[If the request seeks only access, response below is due within 30 days of request without extension.]

The group health plan sponsored by Reliance Steel & Aluminum Co. (“Plan”) has approved your request to access your health information. Accordingly, the Plan will provide access at **[State the manner in which access will be provided]**.

If you have any questions, please contact the HIPAA Privacy Group at **[Insert telephone number]**.

[OR, If the request seeks copies of Protected Health Information, response below is due within 30 days of request without extension.]

The group health plan sponsored by Reliance Steel & Aluminum Co. (“Plan”) has approved your request for copies of your health information and has enclosed the copies requested. The HIPAA Privacy Rule entitles the Plan to be reimbursed for the cost of providing these copies to you. Accordingly, please forward to the address above a check made payable to “**[Insert name]**” in the amount **[\$x.xx]** to cover the cost of providing the copies.

If you have any questions, please contact the HIPAA Privacy Group at **[Insert telephone number]**.

[OR: If Plan needs an extension of time to respond which must be provided within 30 days of the date the request was received.]

The group health plan sponsored by Reliance Steel & Aluminum Co. (“Plan”) received your request for access to health information on _____. The Plan has evaluated your request, however, a delay in action is necessary because **[Describe reason for the delay]**.

The Plan will respond to your request by _____. **[List date that is no later than 60 days from the date of the request.]**

If you have any questions, please contact the HIPAA Privacy Group at **[Insert telephone number]**.

[OR: If Plan denies the request to access, and such denial is not subject to review, the denial must be provided within 30 days of the date the request was received.]

The group health plan sponsored by Reliance Steel & Aluminum Co. (“Plan”) received your request to amend health information on _____. Your request is denied because **[State the basis for the denial]**.

[If the requestor is entitled to a review of the decision, include: (i) a statement that the individual may have the right to have a licensed health care professional, chosen by the Plan, review the denial; and (ii) a description of how the individual may exercise such review rights.]

You may file a complaint regarding this decision with the Plan or the U.S. Department of Health and Human Services. If you file a complaint with the Plan, please file it in writing with the following person: **[State the name or title and telephone number of the contact person designated to receive complaints]**.

If you have any questions, please contact the HIPAA Privacy Group at **[Insert telephone number]**.

7.17 RESPONSE TO INDIVIDUAL'S REQUEST TO AMEND PROTECTED HEALTH INFORMATION

[RELIANCE STEEL & ALUMINUM CO. LETTERHEAD]

[Date]

[Insert individual or personal representative]

[Insert address]

RE: Request to Amend Protected Health Information

Dear [Insert individual or personal representative]:

[If Plan approves the request to amend which must be provided within 60 days of the date the request was received.]

The group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") has approved your request to amend or correct your health information. Accordingly, the Plan will make an appropriate amendment to the Designated Record Set.

You must provide the Plan with the names of any persons to whom you wish to provide the amended information. The Plan then will make reasonable efforts to inform these individuals, as well as any other individuals pursuant to its Privacy Policy.

If you have any questions, please contact the HIPAA Privacy Group at [Insert telephone number].

[OR: If Plan needs an extension of time to respond which must be provided within 60 days of the date the request was received.]

The group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") received your request to amend health information on _____. The Plan has evaluated your request, however, a delay in action is necessary because **[Describe reason for the delay]**.

The Plan will respond to your request by _____. **[List date that is no later than 90 days from the date of the request]**.

If you have any questions, please contact the HIPAA Privacy Group at [Insert telephone number].

[OR: If Plan denies the request to amend which must be provided within 60 days of the date the request was received.]

The group health plan sponsored by Reliance Steel & Aluminum Co. ("Plan") received your request to amend health information on _____. Your request is denied because **[State the basis for the denial]**.

You have the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement must be limited to two single-sided 8-1/2 x 11 pages. **[The length restriction may be established by the plan and must be reasonable.]** The statement of disagreement should be filed within

60 days of this notice with the following office **[List individual or office]**. The Plan has the right to prepare a rebuttal statement to your statement of disagreement. If it does so, you will receive a copy.

If you do not submit a statement of disagreement, you may request that the Plan provide your request for amendment and this denial of amendment with any future disclosures of Protected Health Information that is the subject of this request. You may file a complaint regarding this decision with the Plan or the U.S. Department of Health and Human Services. If you file a complaint with the group health plan, please file it in writing with the following person: **[State the name or title and telephone number of the contact person designated to receive complaints]**.

If you have any questions, please contact the HIPAA Privacy Group at **[Insert telephone number]**.

7.18 DATA BREACH RESPONSE CHECKLIST

Step 1 – Discover Incident

- ☐ Person receiving report of unauthorized access to or acquisition of personal information or protected health information (e.g., data loss/lost or stolen device) must immediately notify Privacy Officer.

Step 2 – Secure Systems

- ☐ Privacy Officer and other appropriate company personnel must immediately take steps to secure company information systems, including any and all files containing claimant, employee and other individuals' personal information or protected health information that may be at risk.
- ☐ Appoint a key person within the company to monitor the progress and communicate the actions as necessary and appropriate.

Step 3 – Make a Preliminary Assessment of the Incident

- ☐ Persons responsible for addressing breach should make the following inquiries concerning the incident:
 - ☐ What devices or paperwork were lost, stolen or breached?
 - ☐ If devices were stolen, was the incident reported to law enforcement? Obtain a copy of police report, if applicable. If the theft has not yet been reported, report immediately. If law enforcement was involved, determine whether law enforcement requires a delay in notification pending investigation and communication to the public.
 - ☐ Interview employees and others involved to determine nature and scope of incident. Require employee(s) and others to prepare report of data maintained on device based on actual knowledge or best recollection. Coordinate with appropriate members of IT to assist in this process, including review of logs of downloaded data.
- ☐ Determine the data elements involved in the incident:
 - a. Individual's name
 - b. Social Security Number
 - c. Financial Account Number
 - d. Driver's License Number
 - e. State Identification Card Number
 - f. Health Information
 - g. Biometric Information
 - h. Home address
 - i. Any other specific information that might identify an individual
- ☐ Determine how many individuals were affected or whose information was compromised by the Incident.

- ☐ Determine what other information may be at risk?
- ☐ Consider whether immediate, preliminary notification to federal and/or state agencies is required.

Step 4 – Coordinate With Appropriate Members of Management; Alert Insurance Company

- ☐ Depending on nature and scope of incident, Privacy Officer shall notify some or all of the individuals listed below with the known details.
 - ☐ Management responsible for the business unit
 - ☐ General Counsel
 - ☐ Risk Management
 - ☐ Chief Information Officer
 - ☐ Public/Claimant Relations
 - ☐ Internal Audit
 - ☐ Human Resources (if data loss involves employee data)
- ☐ Notify carrier that provides data breach insurance.

Step 5 – Further Evaluate the Scope of the Incident

- ☐ If a lost or stolen device, was it encrypted?
- ☐ Does there appear to be evidence of suspicious behavior or negligence by an employee or third party?
- ☐ Is computer forensic expertise needed to complete and validate the investigation? Does the company's IT staff have the appropriate expertise and objectivity to conduct the investigation?
- ☐ Does a backup of the system/data exist?
- ☐ Is there a similar functioning device that can be analyzed to help determine the exposure?

Step 6 – Prepare for and Send Notifications

- ☐ As soon as possible, consult with in-house/outside counsel to determine whether notification is required. Ensure appropriate security agreement is in place with outside counsel. Consider the following issues:
 - ☐ Does HIPAA or other federal breach notification requirements apply?
 - ☐ Which state laws apply?
 - ☐ If persons in other countries are affected, determine requirements under laws in those countries.
- ☐ If the law permits, make a determination of risk of harm. If the Incident involves PHI, conduct an assessment to determine whether a breach under HIPAA has occurred. The analysis

must examine at a minimum, the following four factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person(s) 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. Under HIPAA there is a presumption that a breach occurred when impermissible uses and disclosures of PHI are found. After reviewing these factors, if the Company cannot demonstrate that there is a low probability of compromise to the PHI, or that one of the three specific exceptions under the HIPAA Breach Notification Rule apply, it must provide notification. In lieu of conducting an assessment, the Company can choose to provide notification.

- ☐ How soon must notice be provided?
 - ☐ What does each jurisdiction require to be included in the notification letter?
 - ☐ How may notice be sent? Consider whether a website disclosure would be beneficial to share information with the impacted individuals on the incident and next steps.
 - ☐ What governmental agencies have to be notified? If notification is required to be made to governmental entities, the company must use the forms established by those agencies. (For PHI, determine whether and how the Secretary of HHS needs to be notified).
 - ☐ Whether notification to the media is required. (Under HIPAA media notification is required for breach involving 500 or more residents of a State or jurisdiction).
 - ☐ What if the company does not have current address information?
 - ☐ What types of documentation are required to prove that notifications were given or that the disclosure did not constitute a breach under applicable law?
-
- ☐ Determine whether the company will provide credit monitoring services. Work through legal counsel to engage vendor and coordinate with vendor on letter content and implementation. Ensure appropriate security agreement is in place with credit monitoring vendor.
 - ☐ Involve Public/Consumer Relations in the drafting process and coordinate with legal review.
 - ☐ Determine who will sign notification letter and point of contact for question concerning data breach.
 - ☐ If call center services are obtained, coordinate with call center vendor. Also, establish escalation process to address questions from affected persons that need to be posed to company management. Ensure appropriate security agreement is in place with call center vendor.
 - ☐ Determine whether to make FAQs available to affected persons concerning the incident.

7.19 ASSESSMENT AND IMPLEMENTATION MATERIALS – SELF AUDIT FORM

SELF-AUDIT FORM

[Complete each section below. If not applicable, indicate accordingly]

Name:

Position:

Date:

Plan:

PHI Activity:	Plan eligibility (i.e., determination of eligible employees spouses or dependents)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (i.e., paper, electronically, destroyed):	
List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Plan enrollment or disenrollment (may involve insurability criteria, pre-existing conditions, change in status data, and coordination with Medicare)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (i.e., paper, electronically, destroyed):	
List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Premium/contribution (whether or not pre-tax) payments (technically this information is PHI – likely to arise from enrollment, disenrollment, or mid-year election changes)

What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (<i>i.e., paper, electronically, destroyed</i>):	
List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Health care claims (<i>i.e.</i> , assisting employees with GHP claims and appeals of denied claims that are being improperly denied or not paid - may involve PHI regarding claim)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (<i>i.e., paper, electronically, destroyed</i>):	
List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Referral certification and authorization (medical provider/specialist etc.) (should only apply when employer processes benefit claims; otherwise, will be done by Insurer/TPA)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (<i>i.e., paper, electronically, destroyed</i>):	
List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Medical services or medical care (on or off site)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (<i>i.e., paper, electronically, destroyed</i>):	

List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Auditing vendor activity (e.g., reviewing TPA claims processing activities)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (i.e., paper, electronically, destroyed):	
List administrative, physical and/or technical safeguards in place:	
PHI Activity:	Flexible spending account claims/distributions (should only apply if employer processes claims itself or its employees assist Insurer/TPA)
What PHI is involved:	
How is PHI received and from whom, and who has access:	
How is PHI used and/or shared:	
How is PHI stored (i.e., paper, electronically, destroyed):	
List administrative, physical and/or technical safeguards in place:	

7.20 ASSESSMENT AND IMPLEMENTATION MATERIALS – ADMINISTRATIVE, PHYSICAL AND TECHNICAL CHECKLISTS

ADMINISTRATIVE SAFEGUARDS CHECKLIST

Administrative Safeguards Activity	Details	Implementation Steps Taken or Conclusion That Standard/Specification Is Inapplicable
Security Management Process: Implement policies and procedures to prevent, detect, contain and correct security violation. As set forth under specific implementation standards below.		
Risk Analysis <i>Required</i>	Perform an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by the Plan.	[See Section(s) 3.2.1, and other company policies and procedures]
Risk Management <i>Required</i>	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.	[See Section(s) 3.2 and 6.3, and other company policies and procedures]
Sanction Policy <i>Required</i>	Develop and apply an appropriate sanctions policy against workforce members who fail to comply with the Plan's security policies and procedures.	[See Section(s) 4.6, and other company policies and procedures]
Information System Activity Review <i>Required</i>	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	[See Section(s) 3.2.1, and other company policies and procedures]
Assignment of Security Responsibility <i>Required</i>	Identify the security official who is responsible for the development and implementation of the policies and procedures required under the Security Standards. Must be documented in an official written designation.	[See Section(s) 3.2.2, and other company policies and procedures]
Workforce Security: Implement policies and procedures to ensure that all members of the Plan's workforce who work with EPHI have appropriate access to EPHI, and to prevent those workforce members who do not have access as provided but who work in locations where EPHI might be accessed from obtaining access to EPHI. As set forth under specific implementation standards below.		
Authorization and/or Supervision <i>Addressable</i>	Implement procedures for the authorization and/or supervision of Plan workforce members who work with EPHI or in locations where it might be accessed.	[See Section(s) 1.1, 6.3 and other company policies and procedures]
Workforce Clearance Procedure <i>Addressable</i>	Implement procedures to determine that the access of a Plan workforce member to EPHI is appropriate.	[See Section(s) 1.1, 6.3, and other company policies and procedures]
Termination Procedures <i>Addressable</i>	Implement procedures for terminating access to EPHI when the employment of a Plan workforce member ends or as required by determinations made under the plan's workforce clearance procedure.	[See Section(s) 1.1, and other company policies and procedures]
Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the requirements of the Privacy Rule and the plan. See specific implementation standards below.		
Access Authorization <i>Addressable</i>	Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process or other mechanism.	[See Section(s) 1.1, 6.3, and other company policies and procedures]
Access Establishment and Modification <i>Addressable</i>	Implement policies and procedures that, based upon the Plan's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process.	[See Section(s) 1.1, 6.3, and other company policies and procedures]

Administrative Safeguards Activity	Details	Implementation Steps Taken or Conclusion That Standard/Specification Is Inapplicable
Security Awareness Training: Current members of Plan's workforce will be trained upon implementation of Privacy & Security Procedures. Future members of Plan's workforce will be trained prior to grant of access to EPHI.		
Security Reminders <i>Addressable</i>	Providing periodic security updates (e.g., to address new threats, provide reminders, etc).	[See Section(s) 3.2.3, 4.7, 6.3, and other company policies and procedures]
Protection from Malicious Software <i>Addressable</i>	Providing training on procedures for guarding against, detecting and reporting malicious software.	[See Section(s) 3.2.3, 4.7, and other company policies and procedures]
Log-in Monitoring <i>Addressable</i>	Providing training on procedures for monitoring log-in attempts and reporting discrepancies.	[See Section(s) 3.2.3, 3.3.2, 4.7, and other company policies and procedures]
Password Management <i>Addressable</i>	Providing training on procedures for creating, changing, and safeguarding passwords.	[See Section(s) 1.1, 3.2.3, 3.3.2, 4.7, 6.3, and other company policies and procedures]
Security Incident Procedures: Implement policies and procedures to address security incidents. See specific implementation standard below.		
Response and Reporting <i>Required</i>	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, the harmful effects of security incidents that are known to the GHP; and document security incidents and their outcomes.	[See Section(s) 3.2.4, 7.7, 7.17, and other company policies and procedures]
Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain EPHI. See specific implementation standards below.		
Data Back Up Plan <i>Required</i>	Establish and implement policies and procedures to create and maintain retrievable exact copies of EPHI.	[See Section(s) 3.2.5, and other company policies and procedures]
Disaster Recovery Plan <i>Required</i>	Establish (and implement as needed) procedures to restore any loss of data.	[See Section(s) 3.2.6, and other company policies and procedures]
Emergency Mode Operation Plan <i>Required</i>	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.	[See Section(s) 3.2.6, and other company policies and procedures]
Testing and Revision Procedure <i>Addressable</i>	Implement procedures for periodic testing and revision of contingency plans.	
Applications and Data Criticality Analysis <i>Addressable</i>	Assess the relative criticality of specific applications and data in support of other contingency plan components.	
Additional Safeguards		
Evaluation <i>Required</i>	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Standards and subsequently in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which the plan's security measures and its Security Manual meet the requirements of the Security Standards.	[See Section(s) 3.2.1, and other company policies and procedures]
Business Associate Contracts <i>Required</i>	Amend or restate all contracts with the plan's business associates to incorporate security compliance and incident reporting commitments.	[See Section(s) 1.4, 7.4, and other company policies and procedures]

PHYSICAL SAFEGUARDS CHECKLIST

Physical Safeguards Activity	Details	Implementation Steps Taken or Conclusion That Standard/Specification Is Inapplicable
Facility Access Controls: Implement policies and procedures to limit physical access to the GHP's EPHI and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. See also implementation specifications below.		
Identify each plan sponsor location where EPHI is created, sent, stored or received. <i>Required</i>	Identify work stations, terminals, cubicles, storage facilities, buildings (interior and exterior)	[See Section(s) 3.3.1, 6.3 and other company policies and procedures]
Contingency Operations Procedures <i>Addressable</i>	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. To allow facility access in support of retrieval of lost data.	
Facility Security Plan <i>Addressable</i>	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.	[See Section(s) 1.1, 6.3 and other company policies and procedures]
Access Control and Validation <i>Addressable</i>	Implement policies and procedures to control and validate a person's access to facilities based upon their role or function, including controlling visitor access and controlling access to software programs for testing and revision.	[See Section(s) 1.1, 6.3 and other company policies and procedures]
Maintenance Records <i>Addressable</i>	Implement policies and procedures to document repairs and modification to each physical facility which are related to security (for example, hardware, walls, doors, locks).	[See Section(s) 6.3 and other company policies and procedures]
Workstation Use and Security: Implement policies and procedures that address appropriate access to and use of company workstations that can access EPHI.		
Workstation Use <i>Required</i>	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.	[See Section(s) 1.1, 6.3 and other company policies and procedures]
Workstation Security <i>Required</i>	Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.	[See Section(s) 1.1, 3.3, 6.3 and other company policies and procedures]
Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of the GHP's facilities, and the movement of these items within the facilities. See specific implementation specifications below.		
Disposal <i>Required</i>	Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.	[See Section(s) 3.3.1 and other company policies and procedures]
Media Re-use <i>Required</i>	Implement policies and procedures for removal of EPHI from electronic media before the media are made available for reuse.	[See Section(s) 3.3.1 and other company policies and procedures]
Accountability <i>Addressable</i>	Maintain a record of the movement of hardware and electronic media containing EPHI and any person responsible therefor.	[See Section(s) 3.3.1 and other company policies and procedures]
Data Backup and Storage <i>Addressable</i>	Create a retrievable, exact copy of EPHI, when needed, before movement of equipment containing EPHI.	[See Section(s) 3.2.5 and other company policies and procedures]

TECHNICAL SAFEGUARDS CHECKLIST

Technical Safeguards Activity	Details	Implementation Steps Taken or Conclusion That Standard/Specification Is Inapplicable
Access Control: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been properly granted access rights. See Manual for sample policies and procedures. See specific implementation standards below.		
Assign Password Names and/or Numbers <i>Required</i>	Ensure access to components of information systems containing EPHI is limited to those whose access is for an appropriate plan function, based upon usage of password names and/or numbers.	[See Section(s) 1.1, 3.3.2 and other company policies and procedures]
Establish Emergency Access Procedure <i>Required</i>	To provide access to EPHI during an emergency. For example, the GHP could create a single global password name and/or number with access to all information systems and all information system components for security officer.	[See Section(s) 3.2.6 and other company policies and procedures]
Implement Automatic Logoff Procedures <i>Addressable</i>	For each component of each information system that can be accessed by workforce members, implement procedures that terminate an electronic session after a passage of time of inactivity.	[See Section(s) 3.3.2 and other company policies and procedures]
Implement Encryption and Decryption Protections <i>Addressable</i>	Obtain and install software (e.g., tunnel system) <u>or</u> Set up all communications via attachment documents with password protection arrangement <u>or</u> Apply digital certificates to every user	
Audit Controls <i>Required</i>	Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI	[See Section(s) 1.1, 3.2.1 and other company policies and procedures]
EPHI Integrity: Implement procedures to protect EPHI from improper alteration or destruction. See implementation specification below.		
Mechanism to Authenticate EPHI <i>Addressable</i>	Implement electronic procedures to corroborate that EPHI has not been improperly altered or destroyed.	
Person or Entity Authentication <i>Required</i>	Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed. Possibly establish via password names and/or numbers.	[See Section(s) 1.1, 3.3.2 and other company policies and procedures]
Transmission Security: For each information system and with respect to its transmission of EPHI over an electronic network, implement technical security measures to guard against unauthorized access to EPHI. See implementation specifications below.		
Integrity Controls <i>Addressable</i>	Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed.	[See Section(s) 1.1, 3.2.3, 6.3 and other company policies and procedures]
Encryption <i>Addressable</i>	Implement a mechanism to encrypt EPHI whenever deemed appropriate.	

7.21 TRAINING ACKNOWLEDGEMENT FORM

RELIANCE STEEL & ALUMINUM Co. EMPLOYEE ACKNOWLEDGEMENT: HIPAA TRAINING AND COMPLIANCE

Effective _____, 20__

I acknowledge that I received extensive training from my employer regarding the HIPAA privacy policies and procedures of the health plans sponsored by Reliance Steel & Aluminum Co. on _____, 20__.

I acknowledge that I fully understand those HIPAA privacy policies and procedures, and that all of my questions about those policies and procedures have been answered.

I agree that, as a condition of my employment, I will abide by all of the provisions of those HIPAA privacy policies and procedures, both during and after my employment with Reliance Steel & Aluminum Co.

Finally, I agree to bring to the attention of Reliance Steel & Aluminum Co.'s Privacy Officer any questions I have about the HIPAA privacy policies and procedures, any suggestions I have about improving those policies and procedures, or any suspected violations of those policies and procedures.

Signature: _____

Print Name: _____

Date: _____