COMPLIANCE WITH HIPAA PRIVACY STANDARDS

A. Compliance with HIPAA Privacy Standards

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996.

Certain members of the employer's workforce perform services in connection with administration of the Plan. In order to perform these services, it is necessary for these employees from time to time to have access to Protected Health Information (as defined below).

Under the Standards for Privacy of Individually Identifiable Health Information (45 CFR Part 164, the Privacy Standards), these employees are permitted to have such access subject to the following:

1. General. The Plan shall not disclose Protected Health Information to any member of the employer's workforce unless each of the conditions set out in this Compliance with HIPAA Privacy Standards section is met. 'Protected Health Information' shall have the same definition as set out in the Privacy Standards but generally shall mean individually identifiable health information about the past, present, or future physical or mental health or condition of an individual, including information about treatment or payment for treatment.

2. Permitted Uses and Disclosures. Protected Health Information disclosed to business associates and members of the employer's workforce shall be used or disclosed by them only for purposes of Plan administrative functions. The Plan's administrative functions shall include all Plan payment and health care operations. The terms 'payment' and 'health care operations' shall have the same definitions as set out in the Privacy Standards, but the term 'payment' generally shall mean activities taken with respect to payment of premiums or contributions, or to determine or fulfill Plan responsibilities with respect to coverage, provision of benefits, or reimbursement for health care. 'Health care operations' generally shall mean activities on behalf of the Plan that are related to quality assessment; evaluation, training, or accreditation of health care providers; underwriting, premium rating, and other functions related to obtaining or renewing an insurance contract, including stop-loss insurance; medical review; legal services or auditing functions; or business planning, management, and general administrative activities. Genetic information will not be used or disclosed for underwriting purposes.

3. Authorized Employees. The Plan shall disclose Protected Health Information only to members of the employer's workforce who are designated and are authorized to receive such Protected Health Information, and only to the extent and in the minimum amount necessary for these persons to perform duties with respect to the Plan. For purposes of this Compliance with HIPAA Privacy Standards section, members of the employer's workforce shall refer to all employees and other persons under the control of the employer.

   a. Updates Required. The employer shall amend the Plan promptly with respect to any changes in the members of its workforce who are authorized to receive Protected Health Information.

   b. Use and Disclosure Restricted. An authorized member of the employer's workforce who receives Protected Health Information shall use or disclose the Protected Health Information only to the extent necessary to perform his/her duties with respect to the Plan.

   c. Resolution of Issues of Noncompliance. In the event that any member of the employer's workforce uses or discloses Protected Health Information other than as permitted by the Privacy Standards, the incident shall be reported to the privacy official. The privacy official shall take appropriate action, including:

      i. investigation of the incident to determine whether the breach occurred inadvertently, through negligence, or deliberately; whether there is a pattern of breaches; and whether the Protected Health Information was compromised

      ii. applying appropriate sanctions against the person(s) causing the breach, which, depending upon the nature of the breach, may include oral or written reprimand, additional training, or termination of employment

      iii. mitigating any harm caused by the breach, to the extent practicable

iv. documentation of the incident and all actions taken to resolve the issue and mitigate any damages

v. providing notification in accordance with HIPAA requirements

4. Certification of Employer. The employer must provide certification to the Plan that it agrees to all of the following:

a. not use or further disclose the Protected Health Information other than as permitted or required by the plan documents or as required by law

b. ensure that any agent or subcontractor to whom it provides Protected Health Information received from the Plan agrees to the same restrictions and conditions that apply to the employer with respect to such information

c. not use or disclose Protected Health Information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the employer

d. report to the Plan any use or disclosure of the Protected Health Information of which it becomes aware that is inconsistent with the uses or disclosures hereunder or required by law

e. make available Protected Health Information to individual Plan members in accordance with Section 164.524 of the Privacy Standards

f. make available Protected Health Information for amendment by individual Plan members and incorporate any amendments to Protected Health Information in accordance with Section 164.526 of the Privacy Standards

g. make available the Protected Health Information required to provide any accounting of disclosures to individual Plan members in accordance with Section 164.528 of the Privacy Standards

h. make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from the Plan available to the Department of Health and Human Services for purposes of determining compliance by the Plan with the Privacy Standards

i. if feasible, return or destroy all Protected Health Information received from the Plan that the employer still maintains in any form, and retain no copies of such information when no longer needed for the purpose of 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 unfeasible

j. ensure the adequate separation between the Plan and member of the employer's workforce, as required by Section 164.504(f)(2)(iii) of the Privacy Standards

5. The following members of Northwest Arizona Employee Benefit Trust's workforce are designated as authorized to receive Protected Health Information from Northwest Arizona Employee Benefit Trust (Plan) in order to perform their duties with respect to the Plan:

a. HR/Risk Manager

b. HR Director

c. Benefits Specialist

d. HR Technician

e. HR Administrator

f. Client Wellbeing and Engagement Consultant

g. Client Financial Accounting Manager

h. Account Executive

i. Account Manager

j. Account Assistant

B. Compliance with HIPAA Electronic Security Standards

Under the Security Standards for the Protection of Electronic Protected Health Information (45 CFR Part 164.300 et. seq., the Security Standards), the employer agrees to the following:

1. The employer agrees to implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of Electronic Protected Health Information that the employer creates, maintains, or transmits on behalf of the Plan. Electronic Protected Health Information shall have the same definition as set out in the Security Standards, but generally shall mean Protected Health Information that is transmitted by or maintained in electronic media.

2. The employer shall ensure that any agent or subcontractor to whom it provides Electronic Protected Health Information shall agree, in writing, to implement reasonable and appropriate security measures to protect the Electronic Protected Health Information.

3. The employer shall ensure that reasonable and appropriate security measures are implemented to comply with the conditions and requirements set forth in Compliance with HIPAA Privacy Standards, provisions Authorized Employees and Certification of Employers described above.