PREAMBLE

Wheelchair Express Sioux Falls (the Transport Company) is not considered a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA). That is, as a transportation provider the Company is not directly bound by HIPAA's rules for healthcare providers. However, there are contractual relationships under which the Transport Company is a Business Associate of various Covered Entity clients. As a Business Associate the Company is obligated to comply with HIPAA's Privacy, Security, and Enforcement Rules, as well as the HITECH Act with its Breach Notification Rule, with respect to the Protected Health Information (PHI), electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII) provided by its contracted Covered Entity clients for the fulfillment of its transportation functions. The purpose of the Transport Company's HIPAA Policy is to provide guidance for its operating procedures and to ensure compliance with the HIPAA requirements of its contracted Covered Entity clients.

BUSINESS ASSOCIATE POLICY

The Transport Company may contract with third-party vendors, suppliers, or other service providers, including expert witnesses and consultants, to perform various functions for or on behalf of the Transport Company and its clients. At times, these third parties may require access to or disclosure of PHI that is maintained and/or stored by the Transport Company. These third parties are business associates of the Transport Company. The Transport Company will execute compliant Business Associate Agreements with such third parties and will obtain satisfactory assurances from the same that the business associates will adequately and appropriately safeguard the protected health information of the Transport Company (see **Business Associate Agreement Template**, below).

RISK MANAGEMENT POLICY

1. It is the policy of the Transport Company to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its protected health information (PHI) (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the Transport Company's information security program.
2. Risk analysis and risk management are recognized as important components of the Transport Company's compliance program.
3. The Transport Company performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of PHI.
4. The Transport Company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   A. Ensure the confidentiality, integrity, and availability of all PHI the Transport Company creates, receives, maintains, and/or transmits,
   B. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI,

C. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required, and
D. Ensure compliance by workforce.

5. All Transport Company's workforce members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action, up to and including dismissal.

FACILITY ACCESS

The Transport Company safeguards the confidentiality, integrity, and availability of protected health information (PHI) and further safeguards its business, client, and proprietary information within the Transport Company's information systems/applications by controlling access to the physical buildings/facilities that house such systems/applications. Physical access to the Transport Company's offices is limited to only those authorized in this policy. In an effort to safeguard PHI, the facility(s), and systems/applications from unauthorized access, tampering, and theft, access is allowed to designated areas only to those persons authorized to be in them and with escorts for unauthorized persons. For purposes of this Policy, a "Restricted Area" includes all areas of the Transport Company's offices and shop other than the front lobby, conference rooms, hallways, and garage space.

SYSTEM ACCESS POLICY

It is the policy of the Transport Company to safeguard the confidentiality, integrity, and availability of protected health information (PHI) and business and proprietary information within its information systems by controlling access to these systems/applications. Access to electronic protected health information (ePHI) by all users, including but not limited to workforce members, is allowable only on a minimum necessary basis. The workforce is specifically trained on this point. All users are responsible for reporting an incident of unauthorized use or access of the Transport Company's information systems. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the Transport Company's information systems and are extended even after termination or other conclusion of access.

BREACH NOTIFICATION

When impermissive or unauthorized access, acquisition, use, and/or disclosure of the Transport Company's protected health information occurs, breach notification will be carried out in compliance with Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the regulations promulgated thereunder.

1. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a breach is known to the Transport Company, or, by exercising reasonable diligence would have been known to the Transport Company (includes breaches by the Transport Company's business

associates). The Transport Company shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (e.g., a Business Associate acting as an agent of the Transport Company) of the Transport Company. Following the discovery of a potential breach, the Transport Company shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed by the Transport Company, to have been accessed, acquired, used, or disclosed as a result of the breach. The Transport Company shall also begin the process of determining what external notifications are required or should be made.

2. Breach Investigation: The Transport Company shall name an individual to act as the investigator of the breach (e.g., Security Officer). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the Transport Company as appropriate. The investigator shall be the key facilitator for all breach notification processes to the appropriate entities. All documentation related to the breach investigation, including the risk assessment and notifications made, shall be retained for a minimum of (6) six years.
3. Risk Assessment: For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. An "acquisition, access, use, or disclosure in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:
    A. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    B. The unauthorized person who used the protected health information or to whom the disclosure was made;
    C. Whether the protected health information was actually acquired or viewed; and
    D. The extent to which the risk to the protected health information has been mitigated.
4. The Transport Company shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The Transport Company has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the Transport Company will determine the need to move forward with breach notification. The Transport Company may make breach notifications without completing a risk assessment.
5. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the Transport Company involved or the business associate involved that is acting as the Transport Company's agent. It is the responsibility of the Transport Company to demonstrate that all

notifications were made as required, including evidence demonstrating the necessity of delay.

6. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the Transport Company that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Transport Company shall:
    A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or
    B. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.
7. Content of the Notice: The notice shall be written in plain language and must contain the following information:
    A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
    C. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
    D. A brief description of what the Transport Company is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and
    E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
8. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The Security Officer shall ensure that the appropriate individuals or entities are notified of the Breach.
9. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the Transport Company shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected. The following information should be collected/logged for each breach:
    A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known;
    B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.);
    C. A description of the action taken with regard to notification of individuals, the media, and the Secretary regarding the breach.
    D. The results of the risk assessment; and
    E. Resolution steps taken to mitigate the breach and prevent future occurrences.

10. Business Associate Responsibilities: The Transport Company is a Business Associate of its covered entity clients. In the event of an impermissible use or disclosure of PHI, the Transport Company shall comply with its notification obligations pursuant to HIPAA and any Business Associate Agreements entered into between the Transport Company and its Covered Entity clients. Business associates are now directly liable for impermissible uses and disclosures, provision of breach notification to the covered entity, completing breach risk assessments, breach documentation requirements, and civil and criminal penalties for violations. Any business associate (BA) of the Transport Company that accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the Transport Company of such breach (when the business associate is an agent of the Transport Company, this notification must be provided within a shorter timeframe as specified in the Business Associate Agreement). Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the Transport Company with any other available information that the Transport Company is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the Transport Company will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals.
11. Workforce Training: The Transport Company shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and promptly report breaches within the Transport Company, as well as return or destroy PHI, as appropriate for the incident. Workforce members that assist in investigating, documenting, and resolving breaches are trained on how to complete these activities.
12. Complaints: Individuals have the right to complain about the Transport Company's breach notification processes.
13. Sanctions: The Transport Company shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.
14. Retaliation/Waiver: The Transport Company may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right.

DATA MANAGEMENT – DISASTER RECOVERY – EMERGENCY OPERATIONS

The Transport Company establishes and implements procedures to create and maintain retrievable exact copies of electronic protected health information. The policy and procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all information systems used by the Transport Company. Data back up and the correct storage of backup media are an important part of the day-to-day operations of the Transport Company's information security. To protect the confidentiality, integrity, and availability of ePHI, the Transport Company completes backups to assure that data

remains available when it is needed. Data that are not stored on the Transport Company's own hardware will be stored with vendors who also guarantee the security and retrievability of data.

WORKFORCE TRAINING

The Transport Company trains the members of its workforce regarding the Transport Company's privacy and security obligations of Protected Health Information. All training shall be done upon an employee's initial hire and, subsequently, at least annually.

SANCTION POLICY

The Transport Company will discipline any employees or partners who fail to comply with the Transport Company's HIPAA policies and procedures.