First Transit

HIPAA COMPLIANCE PLAN

FOR

FIRST TRANSIT, INC.

Amended and Restated, Effective June 13, 2014

FIRST TRANSIT, INC.
CORPORATE RESOLUTION

Effective June 13, 2014, First Transit, Inc., on behalf of its para-transit subsidiaries and affiliates (collectively called "First Transit" in this document), adopts this Amended and Restated HIPAA Compliance Plan to ensure the privacy, security, and proper Use and Disclosure of Protected Health Information, in compliance with applicable federal and state law, including the HIPAA Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E) and the HIPAA Security Rule (45 CFR Parts 160 and 164, Subparts A and C) and to satisfy the provisions of the Health Information Technology for Economic and Clinical Health Act, set forth in Division A, Title XIII, of the American Recovery and Reinvestment Act of 2009, and its implementing regulations and guidance (collectively, "HITECH"), including the Final Omnibus Rule. This amended and restated plan replaces the plan adopted effective September 2013 in its entirety.

First Transit Compliance Officer will oversee the company's compliance with the privacy standards under HIPAA, and the HIPAA Security Panel will be comprised of the following: First Transit Compliance Officer; FirstGroup America Director of Security and First Transit's Senior Director of IT.

First Transit

HIPAA COMPLIANCE PLAN

Table of Contents

I. HIPAA Definitions

Access: The ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any system resource.

Authentication: The corroboration that a person is the one claimed.

Authorization: A written form containing the core elements and required statements set forth in the Privacy Rule, which is written in plain language and signed by an Individual to allow a Covered Entity or Business Associate to Use or Disclose Protected Health Information for purposes other than Treatment, payment, and Health Care Operations.

Availability: Data or information is accessible and useable upon demand by an authorized person.

Breach: For purposes of the breach notification provisions of HIPAA, "Breach" means the acquisition, access, Use or Disclosure of Protected Health Information in a manner not permitted, which compromises the security or privacy of the Protected Health Information. For purposes of this definition, "compromises the security or privacy of the Protected Health Information" means "poses a significant risk of financial, reputation or other harm to the Individual."

Business Associate: A person or organization that performs a function, activity or service on behalf of a Covered Entity that creates, received, maintains, or transmits Protected Health Information, such as claims processing, claims administration, data analysis, utilization review, quality assurance, billing, practice management, legal counsel, benefits management, or information technology consultants. It shall also include a subcontractor that creates, receives, maintains or transmits PHI on behalf of a Business Associate.

Business Associate Agreement: A written agreement between a Covered Entity and a Business Associate that guides how the parties will Use and Disclose Protected Health Information to perform the functions and activities of the business relationship in compliance with HIPAA.

Compliance Officer: A person appointed by First Transit to be responsible for ensuring compliance with Privacy Rule through appropriate HIPAA policies and procedures.

Confidentiality: Data or information is not made available or Disclosed to unauthorized persons or processes.

Covered Entity: A Health Plan, Health Care Clearinghouse, or a Health Care Provider that transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulations.

Designated Record Set: A group of records created and/or maintained by a Covered Entity or Business Associate that include medical, billing, and health plan records that may be used in whole or in part to make decisions about Individuals, as defined in the Privacy Rule.

Disclosure: The release, transfer, provision of access to, or divulging in any manner of Individually Identifiable Health Information to any person or entity outside of an entity holding the information.

Electronic Media: Refers to electronic storage media, such as computer memory devices (hard drives) and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Also refers to transmission media used to exchange information contained in electronic storage media, such as internet, extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Transmissions involving paper or voice, such as by fax or telephone, are not electronic media because the information being exchanged did not exist in electronic form before transmission.

Electronic Protected Health Information (ePHI): Protected Health Information that exists or is stored in Electronic Media.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, as defined in the Security Rule.

Facility: The physical premises, including the interior and exterior of an office.

Health Care: Care, services or supplies related to the health of an Individual, including preventive, diagnostic, therapeutic, rehabilitative, maintenance, palliative, and counseling care and services, or the sale of drugs, devices, equipment and other items in accordance with a prescription.

Health Care Clearinghouse: A public or private entity such as a billing service, a re-pricing company, or management and information systems that processes Health Information received from another entity into a HIPAA-compliant transaction for the electronic transmission of that Health Information.

Health Care Provider: A provider of medical or health services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business.

Health Information: Any information, oral or written and maintained in any form or medium, that relates to an Individual's past, present or future physical or mental health or condition; provision of Health Care to an Individual; or past, present or future payment, for the provision of Health Care and is created or received by a Covered Entity, public health authority, employer, life insurer, and school or university.

Health Plan: An Individual or group health plan that provides for or pays the cost of medical care. Health plans include group health plans, health insurance issuers, HMOs, and most federally-funded health benefits programs.

HIPAA: Health Insurance Portability and Accountability Act of 1996. The Privacy Rule, Security Rule, the American Reinvestment and Recovery Act ("ARRA"), Health Information Technology for Economic and Clinical Health Act "(HITECH"), and Final Omnibus Rule will collectively be referred to in this Plan as HIPAA.

Incidental Disclosures: Unintended Disclosures of Unsecured PHI that occur after reasonable safeguards have been taken to protect against unauthorized persons hearing or viewing an Individual's Protected Health Information.

Individual: A person who is the subject of Protected Health Information.

Individually Identifiable Health Information: A subset of Health Information, Individually Identifiable Health Information means demographic information collected from a Individual relating to past, present or future physical or mental conditions and treatments, or payments for treatment, that identifies the Individual or from which there is a reasonable basis to believe that the information can be used to identify the Individual.

Integrity: The property that data and information have not been altered or destroyed in an unauthorized manner.

Malicious Software: Refers to software designed to damage or disrupt a system, such as a computer virus.

Password: The confidential authentication information composed of a string of characters permitting a person to access ePHI.

Personal Representative: A person with the legal capacity to make health care-related decisions on behalf of the Individual (*i.e.* parent, spouse, guardian, executor, power of attorney).

Privacy Rule: The Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, Subparts A and E.

Protected Health Information (PHI): Individually Identifiable Health Information that is transmitted by electronic means, or transmitted or maintained in any other form or medium.

Security (Security Measures): Refers to all administrative, physical, and technical safeguards taken to protect an information system.

Security Incident: The attempted or successful unauthorized Access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Panel: Persons appointed by First Transit to be responsible for the development and implementation of the policies and procedures required for compliance with the Security Rule through appropriate HIPAA policies and procedures.

Security Rule: The Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160 and 164, Subparts A and C.

Standard: A rule, condition, or requirement relating to operational or informational services, procedures, and performance with respect to the privacy and security of Protected Health Information.

Unsecured Protected Health Information: 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 in guidance issued and posted on the HHS website (*i.e.*, encryption and destruction),

Use: The sharing, employment, application, utilization, examination, and analysis of Individually Identifiable Health Information within an entity, such as First Transit, that maintains such information.

User: A person or entity with authorized access to a system, such as a computer.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for First Transit, is under the direct control of First Transit.

Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, and the Electronic Media stored within it and in its immediate environment.

II. HIPAA Officer Job Descriptions

Compliance Officer

The Compliance Officer will oversee First Transit compliance with the Privacy Rule and this Plan and sit on the Security Panel. In this role, the Compliance Officer is responsible for overseeing and assuring proper Access, Use, and Disclosure of Protected Health Information that is generated or maintained by First Transit according to the Privacy Rule and working with the other members of the Security Panel to develop and implement policies and procedures required for compliance with the Security Rule through appropriate HIPAA policies and procedures.

.

The Compliance Officer is also required to have and maintain a good, general and up-to-date understanding of the Privacy Rule and Security Rule, its functional operation and impact on First Transit.

The Compliance Officer's primary duties and responsibilities include:

1. Compliance with the Privacy Rule by First Transit and all Workforce.

2. Overseeing the implementation and enforcement by each region of First Transit privacy and security policies and procedures.

3. Assuring, in conjunction with the Security Panel that reasonable safeguards, security measures, and "firewalls" exist, so that Protected Health Information that is maintained by First Transit is not improperly Used or Disclosed.

4. Assuring, in conjunction with designated Workforce, that reasonable safeguards are maintained and that Protected Health Information that is maintained by First Transit is not improperly Used or Disclosed.

5. Arranging for First Transit to enter into HIPAA-compliant Business Associate Agreements with any Covered Entity on whose behalf First Transmit transmits, creates, receives, or maintains Protected Health Information, and ensuring that the Business Associate Agreements utilized by First Transit are sufficient to address the safeguarding of Protected Health Information.

6. Receiving questions and complaints by Individuals who believe First Transit may have violated their privacy rights under the Privacy Rule, and overseeing First Transit internal complaint resolution process.

7. Overseeing appropriate mitigation and corrective action and recommending disciplinary action (if warranted) if violations of the Privacy Rule occur.

8. Acting as the contact person to respond to questions about First Transit HIPAA practices by the Department of Health and Human Services' Office for Civil Rights.

9. Arranging by each region, business unit or management level for Privacy Rule and Security Rule training for members of the Workforce, who have access to Protected Health Information to perform job duties, when and as required by the Privacy Rule, including maintaining appropriate documentation of such training.

10. Making periodic reports to the Board of Directors and the Workforce about privacy practices, security, and ways to improve them.

11. Maintaining documentation required by the Privacy Rule; and

12. Investigating any issues regarding compliance with the Privacy Rule, Security Rule and Breach Notification Rule.

Security Panel

The Security Panel is responsible for the development and implementation of policies and procedures required for compliance with the Security Rule, which prevent, detect, contain, and correct security violations, as required by the Security Rule. The FirstGroup America Director of Security, Compliance Officer, and Senior Director of IT will comprise the Security Panel.

The Security Panel shall have responsibility for the following duties and responsibilities under the Security Rule:

1. Developing and implementing policies and procedures necessary for compliance with the Security Rule.

    - *Administrative Safeguards:* Implementing policies and procedures to prevent, detect, contain, and correct Security violations (i.e., required safeguards include risk analysis, risk assessment, sanction policy, and information system activity review).
    - *Physical Safeguards*: Implementing policies and procedures to limit physical Access to electronic information systems and the facility in which they are housed while ensuring that properly authorized Access is allowed.
    - *Technical Safeguards:* Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow Access to only those persons or software programs that have been granted access rights.

2. Performing periodic risk analysis and review of First Transit Security and sanctions policies.

3. Ensuring that all members of First Transit Workforce have appropriate Access to ePHI and preventing those Workforce members who do not have Access from obtaining Access to ePHI.

4. Receiving questions and complaints from Individuals who believe First Transit may have violated their Security rights, and in collaboration with the Compliance Officer, overseeing First Transit internal complaint resolution process.

5. Identifying and responding to suspected or known Security Incidents and mitigating, to the extent practicable, harmful effects resulting from Security Incidents that are known to First Transit.

6. Documenting Security Incidents, risk assessment of Security Incidents, investigation, mitigation, and outcomes.

7. Establishing and implementing a contingency plan for emergency or other occurrence (e.g., fire, vandalism, system failure and natural disaster) that damages systems that contain ePHI.

8. Implementing, overseeing, and reviewing First Transit data back-up process, the disaster recovery plan, and the emergency mode operation plan.

9. Addressing whether First Transit should implement procedures for periodic testing and revision of contingency plan and assess the relative criticality of specific applications and data in support of other contingency plan components.

10. Performing a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the Security of ePHI that establishes the extent to which First Transit security policies and procedures meet the requirements of the Security Rule.

11. Providing First Transit Workforce with training, information, and updates about security and threats to Security. Arranging for Security awareness and training for appropriate members of the Workforce, considering the following addressable standards:

    - Providing periodic Security updates and reminders to Workforce and vendors of First Transit.
    - Maintaining procedures for guarding against, detecting, and reporting malicious software (*i.e*. a virus designed to damage or disrupt a system).
    - Maintaining procedures for monitoring log-in attempts and reporting discrepancies.
    - Maintaining procedures for creating, changing, and safeguarding passwords.

12. Establish policies and procedures to manage access and privileges for all system applications, devices that access the system and system users.

13. Maintaining and reviewing physical safeguards, including addressing whether First Transit should establish policies regarding facility access in case of emergency, implement a facility security plan, access control and validation procedures, and maintenance procedures.

14. Overseeing appropriate Workstation Use and Security by First Transit Workforce,

15. Implementing device and media controls, disposal procedures, and Electronic Media re-use and accountability procedures.

16. Working with the Compliance Officer to ensure that the Business Associate Agreements executed by First Transit as well as agreements between First Transit and its subcontractors contain satisfactory assurances to address the safeguarding of electronic Protected Health Information.

17. Working with external vendors to ensure that new hardware and software connected to the existing computer and, if applicable, network system conforms to Security Rule standards and implementation specifications, such as unique user identification, emergency access procedures, automatic logoff, encryption and decryption, audit controls, integrity controls, authentication, and transmission security.

18. Overseeing appropriate corrective action and recommending disciplinary action (if warranted) if violations of the Security Rule occur.

19. Cooperating with the Compliance Officer, who shall have primary responsibility for responding to questions by the Department of Health and Human Services' Office for Civil Rights if an agency investigation is initiated, based on an Individual's complaint.

20. Cooperating with the Compliance Officer, who shall have primary responsibility for responding making periodic reports to First Transit Senior Management, and other appropriate Workforce about HIPAA security practices and ways to improve them.

III. Use and Disclosure of Protected Health Information for Treatment, Payment and Health Care Operations

Policy Statement:

It is the policy of First Transit to comply with HIPAA and to Use or Disclose Protected Health Information as allowed by the Business Associate Agreement and permitted by the Privacy Rule.

HIPAA Requirements:

Under the HIPAA Privacy Rule, First Transit and its Workforce may Use or Disclose an Individual's Protected Health Information (PHI) as allowed by the Business Associate Agreement and permitted by the Privacy Rule without obtaining a separate HIPAA-compliant Authorization from the Individual.

First Transit typically provides paratransit services, non-emergency medical transportation services and/or scheduling services. In this performance of these services, First Transit may receive the PHI of such Individuals. Under the general rule, First Transit may Use or Disclose PHI for:

- Obtaining **Payment** for transportation services provided to Individuals, such as payment from Medicare, Medicaid, private insurers, HMOs, managed care organizations, and related organizations;
- Transportation to Individuals to receive medical treatment or other activities or services relating to an Individual's health care, including sending medical records to physicians and health care providers involved with the Individual's treatment;
- The proper management and administration of First Transit's operations, including but not limited to subcontractors relevant to First Transit's operations
    1. Any subcontractor used by First Transit that creates, receives, maintains or transmits PHI on First Transit's behalf shall agree to the same restrictions and conditions that apply to First Transit with respect to such information and First Transit shall implement a Business Associate Agreement with such sub-contractors.

First Transit Policy and Procedure:

Members of the First Transit Workforce may Use or Disclose an Individual's PHI as necessary to perform his/her assigned work duties with respect to the provision of paratransit services, non-emergency medical transportation and/or scheduling such transportation, which includes obtaining payment for such services and/or arranging for such Individuals to receive treatment.

IV. Use and Disclosure of Protected Health Information by Authorization

Policy Statement:

It is the policy of First Transit to comply with the HIPAA Privacy Rule and to require an Authorization prior to Using or Disclosing any Protected Health Information (PHI) for purposes other than those stated above in Section III of this Policy, unless permitted or required without authorization by the HIPAA.

HIPAA Requirements:

The HIPAA Privacy Rule requires an Individual (or his/her personal representative) to sign an Authorization before First Transit can Use, Disclose, or release Protected Health Information for purposes not related to Treatment, Payment or Health Care Operations, permitted in the Business Associate Agreement or any other purpose for which Disclosure is allowed without an Authorization. See policy regarding Mandatory Disclosure and Reporting Authorization in Section VI.

First Transit Policy and Procedure:

It is the policy of First Transit to rely on the Covered Entity or Business Associate for whom First Transit is performing services to obtain Authorization for Uses and Disclosures, as required by HIPAA. Members of the First Transit Workforce who believe an Authorization is required must notify Compliance Officer and his or her immediate supervisor and shall refrain from Using or Disclosing PHI until receiving further instruction from the Compliance Officer. The immediate supervisor shall also contact the Compliance Officer, who has ultimate authority to determine whether an Authorization is required. No member of the Workforce may request or obtain an Authorization without approval from the Compliance Officer.

V. Use and Disclosure of Protected Health Information
Restrictions on the Sale of PHI and on Uses and Disclosures for Marketing and Fundraising

Policy Statement:

It is the policy of First Transit to comply with HIPAA and its limitations on the Use or Disclosure of Protected Health Information for Marketing, or Fundraising, and the Sale of PHI.

First Transit Policies and Procedures:

First Transit shall not Use or Disclose Protected Health Information for marketing or fundraising and shall not sale Protected Health Information. All questions about the Use or Disclosure of Protected Health Information for such purposes should be directed to the Compliance Officer.

VI. Release or Disclosure of Protected Health Information without Authorization Mandatory Disclosures and Reporting

Policy Statement:

It is the policy of First Transit to comply with both Federal and State laws concerning the mandatory Disclosure of Protected Health Information.

HIPAA Requirements:

An Individual's Protected Health Information may be Used or Disclosed without his or her written Authorization for certain purposes specified in the Privacy Rule such as (a) public health activities; (b) abuse, neglect, or domestic violence; (c) health oversight activities; (d) judicial and administrative proceedings; (e) law enforcement; (f) disclosures regarding decedents; (g) organ donation; (h) serious threats to the public safety or the health of others; (i) specialized government functions; and (j) workers' compensation.

First Transit Policy and Procedure:

First Transit may Use or Disclose Protected Health Information for the reasons outlined above in a manner consistent with HIPAA. The Compliance Officer will make or supervise all Uses and Disclosures for these reasons. To the extent any Disclosure of PHI is made under this Section, the Compliance Officer (or his or her designee) shall log the Disclosure, including a copy of any request for information (*e.g*. court order, subpoena, request from law enforcement or government agency, etc.), the information disclosed, the date of the disclosure, and the person or entity to whom the Disclosure was made.

VII. Release of Protected Health Information to Entities Not Covered by HIPAA Protected Health Information Subject to Re-Disclosure

Policy Statement:

It is the policy of First Transit to comply with HIPAA and Disclose Protected Health Information only as permitted or required by the Privacy Rule.

HIPAA Requirements:

The Privacy Rule requires a valid Authorization before any Protected Health Information can be Disclosed to entities not covered by HIPAA (*i.e.* not a Covered Entity or Business Associate).

Once an Individual's Protected Health Information has been Disclosed to an entity not covered by the Privacy Rule that Protected Health Information may lose the privacy protections secured by the Privacy Rule and is subject to re-Disclosure. For example, the or entity receiving the Protected Health Information may re-Disclose that information to anyone, without the Individual's Authorization.

First Transit Policy and Procedure:

The Compliance Officer will handle or supervise all Disclosures of Protected Health Information not otherwise permitted or required under an existing Business Associate Agreement or HIPAA Subcontractor Agreement. Any such Disclosures shall be made in a manner consistent with HIPAA and shall be documented in the Accounting of Disclosures Log.

VIII. Transmitting Protected Health Information by Fax, E-Mail, Telephone and Machines

Policy Statement:

It is the policy of First Transit to comply with HIPAA's Privacy Rule and to make reasonable efforts to safeguard the privacy and confidentiality of information when transmitting or communicating Protected Health Information.

HIPAA Requirements:

The HIPAA Privacy Rule requires First Transit Workforce to protect the privacy and confidentiality of Protected Health Information. To comply with the Privacy Rule, First Transit uses reasonable safeguards to prevent the unauthorized, improper or unintended Use and Disclosure of Protected Health Information.

First Transit Policy and Procedure:

A. Transmitting an Individual's Protected Health Information by fax

- Check the Individual file to make sure that the Protected Health Information may be faxed to the recipient or whether the Individual has designated an alternative location or alternative means of communication.

- Before sending the fax, check the number to make sure the fax is sent to the correct recipient.

- If a fax is being sent to a recipient who does not usually receive Protected Health Information in this manner, call the recipient before faxing to alert the recipient to the incoming fax.

- Always use a fax cover sheet indicating the proper recipient and a warning that confidential and privileged information may be contained in the attached message.

    1. This fax, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, Use, and Disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by calling (XXX-XXX-XXXX Phone Number) and destroy all copies of the original message

- A copy of the fax transmission report should be placed in the Individual file or HIPAA Fax Transmission file if more appropriate for the specific business.

B. Transmitting an Individual's Protected Health Information by telephone

- Check the Individual file (a) to make sure that First Transit can contact the Individual or other persons by telephone or (b) to determine whether the Individual has designated an alternative location or alternative means of communication. Check also to make sure that a message may be left with a person, on an answering machine, or on voice mail at the telephone number.

- Before placing a telephone call to the Individual or a Health Care Provider, check the number before dialing.

- If the call is answered, ask whether you can speak with the Individual. If the Individual is not available, leave a message for the Individual to call First Transit. Do not leave detailed medical information another person or on an answering machine.

    - *Sample guidelines for messages include:*
        - *"Can you please leave a message that First Transit (or other business name) called for (Individual's Name), and have (Individual's Name) call us back at (XXX-XXX-XXXX phone number)? Thank you."*

- If the call involves a minor, you may speak with the minor's parent unless this communication is not permitted (See Use and Disclosure of a Minor's Protected Health Information herein).

- If the call is answered by an answering machine or voice mail, leave a brief message such as:

    - "This is First Transit calling for (Individual name), please call us back at xxx-xxxx" OR "This is First Transit calling to remind (Individual name) about his/her ride on date at time p.m."

D. Transmitting an Individual's Protected Health Information by E-mail

- Check the Individual file to make sure that First Transit can contact the Individual or other persons by e-mail and to check whether the Individual has designated an alternative location or alternate means of communication.

- Type the e-mail address, and check to make sure the correct address was typed.

- Include the following statement at the beginning of the e-mail:

"This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, Use, and Disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by separate e-mail and destroy all copies of the original message."

IX. Protecting an Individual's Protected Health Information from Incidental Uses and Disclosures

Policy Statement:

It is the policy of First Transit to comply with the Privacy Rule and to take reasonable efforts to safeguard the privacy and confidentiality of Individuals and prevent Protected Health Information from being viewed or overheard by unintended or unauthorized persons.

HIPAA Requirements:

The HIPAA Privacy Rule requires First Transit to take reasonable steps to protect the privacy and confidentiality of all Individuals.

First Transit Policy and Procedure:

A. Conversations with Individuals

No matter where the conversation with an Individual occurs in the office, Workforce members should always be aware of other persons, including other Workforce members, in the same area. If a family member or other person is present, ask the Individual if the family member or other person can hear the conversation.

Reasonable steps should be taken to protect an Individual's privacy, such as moving the conversation to a private room and closing the door; moving the conversation to a low-traffic area; or lowering the volume of voices.

B. Conversations between Workforce members

Remember that not all Workforce members have the same level of access to PHI. Do not assume that you may discuss PHI with your fellow Workforce members. Access to PHI is individually determined at First Transit taking into consideration the Workforce member's role and duties, as well as the specific needs of the business. Conversations with other Workforce members about PHI should **only** occur for specific business functions. HIPAA's Privacy Rule and First Transit's policy prohibits the discussion of PHI for social or non-business purposes.

No matter where the conversation with another Workforce member occurs, both Workforce members should always be aware of the other persons, including other Workforce members, present in the same area. Reasonable steps should be taken to protect an Individual's privacy, such as moving the conversation to a private room and closing the door, moving the conversation to a low-traffic area, or lowering the volume of voices.

C. Records, files and information

Whenever a Workforce member is using a file containing Protected Health Information, he/she should be aware of other persons in the area.

- Never leave an open file on an unattended desk or area.
- Never keep open files on top of the desk when you leave at the end of the day.
- If you have to leave for a short period of time in the middle of a project, turn the page over or use some other means of shielding the Individual's information from others who may unintentionally view it.

Workforce should not share unique IDs, passwords/codes, minimize computer monitors when not actively working on matter, turn monitors away from view of others and log off when not using computers (See Security Standards set forth in Sections XIX - XXII).

Always try to replace an Individual file or other written material in the appropriate storage location as soon as reasonably possible after a task is completed.

An individual's files and records should not be removed from the premises of First Transit without approval of the Compliance Officer. When anyone transports files and records containing Protected Health Information, they are to always use a container with a lid that can be secured. Persons who are not members of First Transit Workforce should never be allowed to transport or have access Protected Health Information.

D. Filing cabinets

Workforce members with access to filing cabinets should always be aware of other persons near or using the filing cabinets. Only Workforce members with access to the filing cabinets should be allowed to obtain or replace materials in the cabinets. Workforce members who have not been granted access should not enter or be allowed to enter the file rooms.

E. Doors and entrances

Doors that do not need to be open should be closed to prevent unauthorized persons from entering First Transit offices.

F. Fax machines and telephones

The fax machine should be placed in a location where incoming documents are not easily viewed by individuals, regardless of whether they are visitors or members of the Workforce.

Check the fax machine several times a day and frequently remove and process incoming faxes containing Protected Health Information.

Telephones should be used in private areas, or behind closed doors, when speaking with Individuals about confidential or private matters.

G. Document Destruction

Do not place documents containing Protected Health Information in the regular trash. All documents containing Protected Health Information, that are not securely kept for businesses purpose, must be placed in the appropriate shred bin or document destruction bin and disposed of in a confidential manner.

When appropriate and feasible, First Transit will utilize the services of a document destruction company. Destruction certificates will be maintained by the Location Manager and available to the Compliance Officer upon request. The Compliance Officer will determine whether it is necessary to have a written agreement with the document destruction company to further protect the confidentiality and security of Protected Health Information as required by HIPAA.

The shred bins and/or document destruction bin will be kept locked at all times.

X. Minimum Necessary Standard

Policy Statement:

It is the policy of First Transit to comply with the Privacy Rule and follow the Minimum Necessary Standard when Using or Disclosing Protected Health Information.

HIPAA Requirements:

The Minimum Necessary Standard requires First Transit to make reasonable efforts to Use or Disclose only the amount of an Individual's Protected Health Information that is necessary for the purpose of the Use or Disclosure to be accomplished.

The Minimum Necessary Standard does not apply to:

- Disclosure to the Individual;
- Disclosures made for treatment purposes;
- Uses or Disclosures made pursuant to an Authorization (however, only the Protected Health Information authorized for Use or Disclosure by the Individual may be released);
- Disclosures made to the Secretary of the Department of Health and Human Services for purposes of determining compliance with the Privacy Rule;
- Uses and Disclosures that are required by Federal or State law; and
- Uses and Disclosures required for First Transit to comply with HIPAA.

First Transit Policy and Procedure:

A. Limitations for Workforce Access

To comply with the Minimum Necessary Standard, First Transit will identify those Workforce members who need access to Protected Health Information to perform their job duties. First Transit will also make reasonable efforts to limit the access of Workforce to Protected Health Information to the minimum necessary amount required to accomplish job-related tasks.

Each Workforce member will learn about his/her ability to access Protected Health Information, if any, during the new employee orientation.

Questions concerning the Minimum Necessary Standard should be directed to the Compliance Officer.

B. Uses within First Transit

For any Uses occurring on a routine and daily basis, all Workforce with access to Protected Health Information will follow these criteria:

- Use only the Protected Health Information in an Individual's record or file that is necessary to accomplish the specific task;
- Do not browse through an Individual's record or file unless the particular task requires information located throughout the Individual's file;
- Once the particular task is completed, scan the information into the Individual file and place the paper copy of the information back into the shred bin; and
- Do not share Protected Health Information with Workforce who do not need it to perform their job duties.

C. Disclosures to Requests

- All requests for Disclosure of Protected Health Information will be reviewed by the Workforce on a case-by-case basis. The Minimum Necessary Standard also applies to Disclosures to other Business Associates and subcontractors.

- The Workforce may rely on a request for Disclosure of Protected Health Information as meeting the Minimum Necessary Standard if the request is reasonable under the circumstances.

- Workforce must limit any Disclosure in response to a request for Protected Health Information to that amount which is reasonably necessary to accomplish the purpose for which the request is made.

D. Requests for an Individual's Entire Record or File

- Generally, First Transit will not have or maintain an Individual's entire record. As a practical matter, First Transit may only have a limited number of documents regarding an Individual. Nonetheless, Workforce may not Disclose an Individual's entire record or file unless the request is specifically justified as the amount of information that is reasonably necessary to accomplish the purpose of the Disclosure or request.
- Workforce may not Use or request an Individual's entire record or file from a Covered Entity, other Business Associate, or subcontractor unless the request is specifically justified as the amount of information that is reasonably necessary to accomplish the purpose of the Use or request (*e.g.*, for treatment purposes).

XI. Use and Disclosure of a Minor's Protected Health Information

Policy Statement:

It is the policy of First Transit to comply with the Privacy Rule and State law and to Use and Disclosure a minor Individual's Protected Health Information.

HIPAA Requirements:

Parents or legal guardians of minor or unemancipated children may make decisions about a child's health care and subject to State law, access a child's health care records and exercise HIPAA privacy rights on behalf of the child. The Privacy Rule ensures that parents will have appropriate access to Health Information about their children. Generally, parents will be able to Access the Health Information of their children, in addition to exercising control over it, unless State law prohibits such Access and control.

If a minor is emancipated, or has the lawful authority to make decisions, then the minor may make decisions concerning his/her Protected Health Information, if he/she consents to the Health Care Service. A minor may also make Health Care decisions with respect to his/her Protected Health Information, if:

- A minor may obtain Health Care Services under State law without parental consent. If a minor consents to Health Care Services, a parent (or the parent's insurer) may not be liable for charges incurred by the minor accessing the services.
- The parent(s) or legal guardian(s) consents to an agreement of confidentiality between the physician and the minor Individual.

The Protected Health Information of a minor may also be Disclosed without either the minor's Authorization or the parent's Authorization for the same reasons as those affecting adult Individuals (see Use and Disclosure of Protected Health Information Without an Authorization for further information).

First Transit may also deny a parent's request to Access or receive the Protected Health Information of a minor if the decision to deny is made by a licensed Health Care Provider in the exercise of professional judgment.

First Transit Policy and Procedure:

It is the policy of First Transit to rely on the Covered Entity or Business Associate for whom First Transit is performing services to inform First Transit of any Restrictions in the Use or Disclosure of certain health information or records as requested by the minor Individual. For Uses or Disclosure of Minor's information and any Termination of such Restrictions or Notice thereof.. Workforce Member should reference their location's specific guidelines regarding HIPAA Use or Disclosure of Minor's PHI.

. Members of the First Transit Workforce who receive a Request to Restrict Use or Disclosure From regarding a Minor's PHI must notify Compliance Officer and his or her immediate supervisor and shall refrain from Using or Disclosing PHI until receiving further instruction from the Compliance Officer. The immediate supervisor shall also contact the Compliance Officer, who has ultimate authority to determine whether an Authorization is required. No member of the Workforce may act of a Request to Restrict without approval from the Compliance Officer.

XII. Disclosure of Protected Health Information to Family Members or Personal Representatives

Policy Statement:

It is the policy of First Transit to comply with the Privacy Rule and State law and to Disclose Protected Health Information to the family members or personal representatives of Individuals only as permitted by the Privacy Rule and State law.

HIPAA Requirements:

First Transit may generally Use or Disclose Protected Health Information to notify family members, personal representatives, relatives, close personal friend or other persons involved in the individuals care about the Individual's location, general condition to the extent relative to his/her transportation, or death.

How an Individual's Protected Health Information is Disclosed to others depends upon whether the Individual is present, if the Individual has signed an Authorization permitting Disclosure, or if the Disclosure is required for an emergency or disaster relief purposes.

First Transit Policy and Procedure:

A. If the Individual is present

Ask the Individual whether his/her Protected Health Information may be Disclosed to the accompanying family member or other person. If the Individual agrees or does not object, or the member of First Transit Workforce making the Disclosure reasonably infers from the circumstances that the Individual does not object, the Disclosure may be made.

B. If the Individual is not present or is incapacitated and in emergency situations

1. Incapacitated. First Transit may Disclose the Protected Health Information if, in the exercise of professional judgment, it is determined that such a Disclosure is in the best interests of the Individual and it is directly relevant to the family member's or other person's involvement in the Individual's health care.

2. Best Judgment. First Transit may use professional judgment and allow, if in the Individual's best interests, a family member, personal representative, relative, friend or other person to act on behalf of the Individual for purposes of picking up prescriptions, x-rays, medical supplies, and other similar forms of Protected Health Information.

1. Disaster relief. First Transit may Disclose Protected Health Information to a public or private entity to assist in disaster relief efforts for purposes of coordinating notification efforts directed at family members, personal representatives, and other persons, unless the Individual objects to the Disclosure or the Disclosure is not in the Individual's best interests.

XIII. Individual Rights Under the Privacy Rule

Policy Statement:

It is the policy of First Transit to comply with the Privacy Rule and, to the extent applicable to Business Associates, allow Individuals to exercise their Individual privacy rights.

General Policy:

Under the Privacy Rule, Individuals have various rights regarding their Protected Health Information, which include the right to:

- limit the Use or Disclosure of their PHI;
- request that communications to them about their PHI be conducted by alternative means or at alternative sites,
- access their PHI;
- amend or correct any inconsistencies or inaccuracies in their PHI;
- and request an accounting of the Disclosure of their PHI.

First Transit shall act in accordance with the requirements of HIPAA regarding these rights. Individuals seeking to exercise these rights will typically contact the Covered Entity, for whom First Transit is performing services as a Business Associate, directly. To the extent an Individual submits a request regarding his/her rights to First Transit, First Transit will send the request to the appropriate Covered Entity immediately. In addition, the Workforce member who receives the request on First Transit behalf shall notify the Compliance Officer immediately so the Compliance Officer can determine what, if any, action is required by First Transit.

XIV. Request for an Accounting of Disclosures

HIPAA Requirements:

Under the Privacy Rule, an Individual (or his/her Legal Representative) has the right to request an accounting of the Disclosures of his/her Protected Health Information made by a Covered Entity (or its Business Associate or subcontractor) during the previous six (6) years.

An accounting does not include the following Disclosures:

- To carry out Treatment, Payment and Health Care operations;
- Directly to the Individual or his/her Personal Representative;
- Incident to a Use or Disclosure permitted by the Privacy Rule;
- In response to an Authorization;
- To include the Individual in a facility directory;
- To persons involved in the Individual's care or for notification purposes; and
- To correctional institutions or law enforcement officials.

An accounting of Disclosures must include the following information:

- The date that Protected Health Information was Disclosed;
- The name and address of the entity or person receiving the Protected Health Information, if known;
- A brief description of the Protected Health Information that was Disclosed;
- A brief statement of the purpose of the Disclosure that reasonably informs the Individual of the basis for the Disclosure, or a copy of the written request to use the Protected Health Information as required by the Secretary, Department of Health and Human Services, or a copy of the request for the Protected Health Information for which an Authorization is not required. (See Mandatory Disclosures and Reporting Policy in Section VI.);
- The frequency, periodicity or number of Disclosures made to the person or entity; and
- The date of the last Disclosure occurring in the accounting period if multiple Disclosures were made to a single person or entity.

First Transit Policy and Procedure:

A. Any request from a Covered Entity or its Business Associate for information to respond to a Request for an Accounting of Disclosures should be sent to the Compliance Officer immediately.

B. The Compliance Officer or his/her designee should review the request to ascertain what, if any, information should be Disclosed to the Covered Entity or Business Associate to satisfy First Transit obligations under HIPAA.

D. If the Compliance Officer determines that a response is required, the Compliance Officer or his/her designee should prepare the accounting of Disclosures as described in the policy above. Any response should be provided in 30 days to ensure a timely response.

F. A copy of the accounting should also be placed in the compliance file maintained by the Compliance Officer.

XV. Business Associate Agreements

Policy Statement:

In connection with the provision of paratransit services, non-emergency medical transportation services and scheduling services , First Transit will enter into Business Associate Agreements in compliance with HIPAA.

HIPAA Requirements:

As a Business Associate, First Transit must enter into written agreements with Covered Entities that have engaged First Transit to perform services, and the performance of such services requires First Transit to have access to Protected Health Information (in written, oral, and/or electronic form). Such agreements shall outline the permitted and required Uses and Disclosures of Protected Health Information. In addition, First Transit is required to enter into agreements with all of its subcontractors who will Access, Use, or Disclose Protected Health Information as part of their services for, or on behalf of, First Transit, in its capacity as a Business Associate. The contract may not authorize First Transit or any of its subcontractors to Use or further Disclose the information in a manner that would violate HIPAA, if done by the Covered Entity.

If First Transit learns of a pattern of activity or conduct by any subcontractor that is a material breach or violation of the subcontractor's obligations under its written agreement with First Transit, First Transit must notify the subcontractor of such breach so subcontractor may take reasonable steps to cure such breach or end the violation, as applicable. If such steps are unsuccessful, First Transit must terminate its contractual arrangement with the subcontractor, if feasible.

First Transit Policy and Procedure:

First Transit has adopted the model agreements for use with covered entities and subcontractors, which shall be available from the Compliance Officer upon request and shall require the approval of Legal prior to execution.

A copy of all Business Associate Agreements and HIPAA Subcontractor Agreements entered into by First Transit shall be maintained by the Compliance Officer.

XVI. Complaint Resolution Procedure

Policy Statement:

It is the policy of First Transit to comply with HIPAA and provide our Individuals with a grievance process in which they can submit complaints and questions concerning First Transit Privacy and Security practices.

HIPAA Requirements:

As a Business Associate under the HIPAA Privacy Rule, First Transit may provide Individuals with a grievance process that they can use to make complaints concerning First Transit privacy policies and procedures for protecting privacy and confidentiality or suspected violations of their privacy or security rights.

First Transit must take all reasonable and necessary steps to promptly resolve any complaints made by Individuals about its policies and procedures. First Transit must also inform all Individuals that make a compliant of their right to complain to the Department of Health and Human Services.

First Transit Policy and Procedure:
Responding to a Complaint

A. If an Individual, or other person, contacts First Transit to make a complaint, provide the Individual with the Complaint Form (by fax, mail, or e-mail) (see Form No. 1).

B. If the Individual, or other person, wants to submit a complaint orally (by telephone or in person), refer the Individual to the Compliance Officer.

C. Assure the Individual, or other person, that his/her Complaint will be promptly investigated. Inform the Individual that First Transit will respond to the complaint within 30 days.

D. The Compliance Officer or his/her designee will record all complaints using the Complaint Record and Disposition Form (Form No. 2) and include:

- The date the complaint was received, nature of the complaint;
- The date when violation allegedly occurred;
- Name of person(s) who allegedly violated the Individual's privacy or security right;
- Description of the investigation;
- Any actions taken; and
- Description of the correspondence or feedback provided to the Individual.

E. The Compliance Officer or his/her designee will analyze the complaint by interviewing the Individual or Workforce members involved, and other methods of investigation as necessary and appropriate.

F. If the complaint is identified (if the Individual or person identifies himself), the Compliance Officer will provide the Individual or person with a letter summarizing the results of the investigation and may include the remedial actions taken by First Transit in response to the Individual's complaint.

G. If the complaint is validated, the Compliance Officer will implement the appropriate and reasonable remedial actions to resolve the complaint. This may entail revising First Transit policies and procedures, job responsibilities, or other functions.

H. If the Individual's complaint is not substantiated by First Transit, the Compliance Officer will send a letter to the Individual summarizing the results of the investigation and an explanation why action cannot be taken in response to the Individual's complaint.

I. The Compliance Officer will inform the Individual, whether the complaint is validated or not, that he/she may also submit a complaint to the Secretary, Department of Health and Human Services and will provide the Secretary's address in any letter sent to the Individual.

J. A statement should be included in all letters to Individuals making complaints:

"Because we understand your concerns about the privacy and confidentiality of medical and health information, it is the policy of First Transit not to retaliate against any Individual making a complaint directly to us or to the Secretary, Department of Health and Human Services."

K. A copy of the Individual's complaint should not be placed in the Individual file. Instead, a copy of the Individual's complaint, along with any follow-up letters and investigation documentation, should be kept in a separate HIPAA-compliance file and the Complaint Log, maintained by the Compliance Officer.

Responding to a Concern About Retaliation

A. First Transit prohibits its Workforce from retaliation against any Individuals who file a complaint using First Transit Complaint Resolution Procedure or submits a complaint to the Secretary, Department of Health and Human Services.

B. Workforce members who retaliate against an Individual, or the Individual's personal representative or family members, may be subject to disciplinary measures as set forth in the Employee Handbook.

C. If an Individual, or other person, voices his/her concern about the potential of retaliation for submitting a complaint, inform the Individual about First Transit policy against retaliation.

D. If the Individual, or other person, needs to speak with someone about his/her concerns, refer the Individual to the Compliance Officer.

XVII. Workforce Confidentiality Agreement

Policy Statement:

It is the policy of First Transit to require all Workforce members to comply with HIPAA and to adhere to the privacy and security policies of First Transit.

HIPAA Requirements:

First Transit and its Workforce must comply with HIPAA.

First Transit Policy and Procedure:

As a part of First Transit commitment to protecting the privacy and security of Individuals' Protected Health Information, Workforce members at HIPAA locations or with access to PHI are required to sign and abide by a Confidentiality Agreement.

By signing the Confidentiality Agreement, the Workforce member agrees to:

- Use and Disclose Protected Health Information only as set forth in First Transit's privacy and security policies and procedures;
- Only access the Protected Health Information needed for his/her job responsibilities, and not to go beyond the access granted in his/her job description (either expressed or based upon reasonable inference);
- Take reasonable steps to safeguard and protect the Privacy and Security of an Individual's Protected Health Information;
- Report suspected and actual violations, Privacy Breaches, Security Incidents, and Breaches of Unsecured Protected Health Information; and
- Maintain and protect the Privacy and Security of all Individuals while a member of the Workforce and after his/her relationship with First Transit ends.

First Transit Policy and Procedure:

A. All Workforce members at HIPAA locations or with access to PHI shall sign the Confidentiality Agreement and shall participate in HIPAA education and training as required by the HIPAA Privacy and Security Rules, as amended from time to time.

B. A copy of the signed Confidentiality Agreement will be placed in the Workforce member's personnel file.

C. The original signed Confidentiality Agreement shall be placed in the HIPAA compliance file maintained by the Compliance Officer.

D. If the Confidentiality Agreement is revised in any material manner, all Workforce members shall be trained as to the revisions and required to sign the revised Confidentiality Agreement.

XVIII. Duty of Workforce to Report Privacy Breaches

Policy Statement:

It is the policy of First Transit to maintain compliance with HIPAA and require its Workforce to report all known or suspected Privacy Breaches promptly to the Compliance Officer.

HIPAA Requirements:

HIPAA requires members of the First Transit Workforce who need access to Protected Health Information to be knowledgeable about protecting the privacy and confidentiality of Individuals and about their duty to report any known or suspected Breaches or violations of an Individual's privacy.

First Transit Policy and Procedure:

A. Workforce members must report, verbally or in writing, any Breach of privacy, or a concern about the privacy or confidentiality of Protected Health Information to the Compliance Officer.

B. All reports will be kept confidential.

C. Anonymous reporting may be made through First Transit's hotline or via e-mail at hotline@FirstGroup.com Attn: HIPAA Compliance Officer.

XIX. Security Standards: General Rules

Policy Statement:

To comply with the HIPAA Security Rule and its standards, First Transit will develop and implement policies, procedures and practices to safeguard Electronic Protected Health Information (ePHI) as provided in the Security Rule's implementation specifications according the following general rules.

HIPAA Requirements and First Transit Policies:

A. General Requirements

1. First Transit will ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, transmits, and maintains.

2. First Transit will protect against any reasonably anticipated threats or hazards to the security and integrity of its ePHI.

3. First Transit will protect against any reasonably anticipated Uses or Disclosures of ePHI that are not permitted, authorized or required by law.

4. First Transit will ensure that all members of its Workforce at HIPAA locations or with access to PHI comply with its HIPAA Security Policies.

B. Flexibility

1. First Transit will determine what security measures it will need to comply with the Security Rule's standards and implementation specifications. To determine which security measures it will use, First Transit will take into account the following factors:

   (a) The HIPAA location's size, complexity and capabilities;

   (b) The HIPAA location's technical infrastructure, hardware, and software security capabilities;

   (c) The cost of the security measures; and

   (d) The probability and criticality of potential risks to ePHI.

C. Implementation Specifications

1. First Transit will adopt policies and procedures for implementation specifications that are designated as:

- **(R)** – Means First Transit is **required** to comply with and implement the Security Rule's implementation specification.

- **(A)** – Means the Security Rule's implementation specification is **addressable**. If a implementation specification is addressable, First Transit must:

    (a) Assess whether the implementation specification is a reasonable and appropriate safeguard in First Transit's particular environment, when analyzed with reference to its likely contribution to safeguarding electronic protected health information and Individuals' identities;

    (b) Implement the implementation specification if reasonable and appropriate.

    (c) If the implementation specification is not reasonable and appropriate, document why it is not reasonable and appropriate for First Transit. Maintain such documentation in First Transit's compliance records.

    (d) If an equivalent alternative measure is reasonable and appropriate, First Transit should implement such measure.

D. Maintenance

First Transit will review and modify security measures and policies as needed after implementation to continue the provision of reasonable and appropriate protection of ePHI and Individuals' identities.

XX. Administrative Safeguards

Policy Statement:

It is the policy of First Transit to take administrative actions to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of First Transit Workforce as relating to the protection of that information to comply with the HIPAA Security Rule.

HIPAA Requirements and First Transit Procedures:

A. Security Management Process

First Transit will implement policies and procedures to prevent, detect, contain, and correct security violations.

1. Risk Analysis **(R)**

First Transit will conduct accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the location.

(a) A risk assessment will be conducted to determine the Access to and Use and Disclosure of ePHI and Individuals requiring access to ePHI in the First Transit facilities and/or workforce. The risk assessment will:

- Identify the scope of the analysis;
- Gather information and data;
- Identify and document potential threats and vulnerabilities to ePHI and identity theft;
- Assess First Transit's current security and protection measures;
- Determine the likelihood that a threat to ePHI will occur;
- Determine the potential impact if a threat occurred;
- Determine the level of risk; and
- Identify the appropriate Security measures that should be taken to protect against threats and risks to EPHI.

(b) The Security Panel or designee will conduct periodic risk assessments to monitor compliance with the Security Rule, determine whether policies and practices require changes, and to analyze any new or modified Security needs. This risk assessment may, but is not required to, be conducted during the company's review of its overall information systems.

(c) All risk assessments will be documented and maintained in First Transit compliance files maintained by the Security Panel or designee.

2. Risk Management **(R)**

First Transit will implement policies and procedures for maintaining the Security of ePHI and Individuals' identities, in addition to adopting adequate security measures to reduce risks and vulnerabilities to a reasonable and appropriate level. First Transit will strive to ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits. First Transit will address potential risks and vulnerabilities identified in Risk Analysis as part of Risk Management.

At times, First Transit may receive e-PHI in connection with the performance of services for a third party. Any such e-PHI will be stored, and if required, transmitted in a secure manner.

To manage risks and to address issues arising from periodic risk assessments, First Transit will:

(a) Develop and implement a risk management plan;

(b) Implement security measures;

(c) Evaluate whether Security measures are appropriate, reasonable, and effective;

(d) Require all Workforce members who have access to e-PHI to perform their job duties to abide by the First Transit Security policies; and

(e) Consult with appropriate software/hardware vendor(s) to appropriately and adequately address risks and vulnerabilities to the ePHI that is stored in First Transit computer and/or network systems.

3. Sanction Policy **(R)**

First Transit will impose appropriate sanctions on Workforce members (employees, volunteers, contractors, etc.) who fail to comply with Security policies and procedures. Possible sanction include disciplinary action as reflected in the Employee Handbook including possible termination of employment.

4. Information System Activity Review **(R)**

First Transit will regularly review records of information system activity, and maintain records of Security incidents, actions, and outcomes.

(a) First Transit will perform periodic audits of electronic media access and use by Workforce members, internally and in collaboration with external vendor(s) and auditors. The Security Panel or designee will maintain records of such audits, findings and response(s).

(b) The Security Panel or designee will document and maintain records of security incident, actions taken, and outcomes.

B. Workforce Security

First Transit will implement procedures to (a) ensure that all members of the Workforce who must access e-PHI to perform their job duties have appropriate access to ePHI and (b) to prevent those Workforce members who do not need access to ePHI from obtaining access to ePHI.

ePHI may be accessed by the Compliance Officer, Security Panel, providers, billing personnel and vendors, and those authorized by the Compliance Officer

1. Authorization and/or Supervision **(A)**

The Security Panel, in collaboration with the Compliance Officer, will establish and implement policies to:

(a) Identify those Workforce members who need access to e-PHI for the performance of job duties.

(b) Supervise access, Use, and Disclosure of ePHI.

(c) Review periodically the authorization of Workforce members to determine whether changes or updates are necessary.

(d) Limit physical access to areas where ePHI may be accessed to Workforce members with proper clearance when possible.

2. Workforce Clearance Procedure **(A)**

The Security Panel, in collaboration with the Compliance Officer, will establish and implement policies to ensure that on the date of hire for a new employee or other Workforce member or on the date of a change in employment or position within First Transit for an existing employee, the employee's or member's manager , will:

(a) Assess the Workforce member's need to access, Use, and Disclose ePHI.

(b) If practicable, assign the Workforce member a unique user identification (user ID), password, and level of access.

(c) Inform the Workforce member about his/her level of access to ePHI, including any areas of restricted access.

(d) Provide the Workforce member with appropriate passwords and other security clearance as necessary.

(e) Review periodically all Workforce members' access rights to ePHI to determine whether modification is necessary. A review will consider whether access should be granted, should be restricted or not granted, or

should be removed if a Workforce member does not have clearance or a need to access the ePHI.

3. Termination Procedures **(A)**

The Security Panel, in collaboration with the Compliance Officer, will establish and implement policies to ensure that upon a Workforce member's termination, or upon any other event that changes a Workforce member's job duties with First Transit, the Security Panel and Compliance Officer will:

(a) Review the Workforce member's clearance and access rights.

(b) Remove the Workforce member's ability to access ePHI, such as terminating the Workforce member's user identification (ID) and password.

(c) Require the Workforce member to return all keys, access cards, equipment, transportable disks and files, and other materials that are the property of First Transit.

C. Information Access Management

First Transit will implement policies and procedures for authorizing Access to ePHI.

1. Access Authorization **(A)**

First Transit will use the following steps for granting Access to ePHI:

(a) Determine the Workforce member's level of Access by job position and need to Access ePHI to complete job functions.

(b) If practicable, provide a Workforce member with the appropriate user ID and passwords to Access only those areas of ePHI required to perform his/her job functions.

(c) Depending upon the Workforce member's position with First Transit, he /she may Access ePHI at his/her workstation.

2. Access Establishment and Modification **(A)**

The Security Panel and Compliance Officer and if necessary, other designees, will implement First Transit Access authorization policies and require managers to document, review, and modify a Workforce member's right of Access to ePHI according to both the procedures set forth in these security policies and First Transit employee policies.

D. Security Awareness and Training

First Transit will implement a Security awareness and training program for all Workforce members who have access to e-PHI, including management, and periodically update such awareness and training.

1. Security Reminders **(A)**

   (a) Periodic updates about Security issues will be provided to Workforce members utilizing presentations and written materials including e-mail and intranet postings.

   (b) Periodic Security updates and notices may also be posted on bulletin boards or other locations on First Transit premises.

   (c) Security updates and information will be provided at staff meetings.

2. Protection from Malicious Software **(A)**

First Transit will adopt methods to guard against, detect, and report malicious software (*i.e.* a virus designed to damage or disrupt a system):

   (a) Use of various software or other application installed in First Transit information systems to protect ePHI.

   (b) Enforce an Electronic Use Policy.

E. Security Incident Procedures

First Transit will implement procedures for addressing Security Incidents.

1. Response and Reporting **(R)**

First Transit will identify and respond to suspected or known Security Incidents and mitigate, to the extent practicable, harmful effects resulting from Security Incidents that are known to First Transit.

   (a) All Workforce members must immediately report any suspected or known Security Incidents, such as virus contamination, unauthorized Access by a Workforce member, Access by any other person, loss of ePHI, or disruption to ePHI to the Security Panel or Compliance Officer.

   (b) The Security Panel or other designated person will investigate the report of a Security Incident using the appropriate form (see Security Incident Report form).

   (c) The Security Panel in collaboration with the Compliance Officer, will determine the appropriate method to address or mitigate the Security Incident.

(d) All efforts to investigate, address, and mitigate will be documented, along with the outcome of the Security Incident. All Security Incident Report forms will be maintained by the Security Panel for First Transit compliance file.

F. Security Contingency Plan

First Transit will establish, and implement as necessary, policies and procedures for responding to an emergency or other occurrence (i.e. fire, vandalism, system failure, and natural disaster) that damages computer and/or network systems containing ePHI. Such policies will include a data backup plan and disaster recovery plan.

1. Data Back-Up Practice **(R)**

First Transit will establish and implement procedures to create and maintain retrievable exact copies of ePHI by:

(a) When needed, copying ePHI onto transportable media (such tape, CD-ROM, paper, or other storage device) and sending it to a secure offsite storage location.

(b) Following First Transit data backup and storage Practice.

(c) Complying with First Transit Device and Media Controls as outlined in Section XVIII(D).

2. Disaster Recovery Practice **(R)**

First Transit will attempt to recover any data losses by:

(a) Timely obtaining stored back-up and re-loading onto to First Transit information systems, network, or computers.

(b) Consulting with an appropriate external vendor to determine the best method for recovering data losses.

3. Emergency Mode Operation Practice **(R)**

In the event of an emergency that disrupts First Transit Electronic Media, First Transit will continue with its critical business processes to the extent practicable and for protection of the Security of ePHI while operating in emergency mode by:

(a) Determining the critical operations and activities of First Transit, if any, that must continue to function during the emergency and disruption.

(b) Continuing with critical operations using alternate methods or locations. For example, paper and other available media will be used until the data and information can be transferred to First Transit electronic records.

(c) Using generators for continued power and other similar measures, if necessary.

(d) The Security Panel and Compliance Officer will determine the best course of action if the emergency threatens First Transit Electronic Media or ePHI.

4. Testing and Revision Procedure **(A)**

The Security Panel, or other designated person, will periodically review First Transit practices and action steps for emergency mode operations. External vendor(s) may be consulted to review First Transit action steps for safeguarding and securing the confidentiality and integrity of ePHI.

5. Applications and Data Criticality Analysis **(A)**

The Security Panel will periodically analyze First Transit action plan and steps for emergency mode operations of its information systems. External vendor(s) may be consulted to review the First Transit action steps for safeguarding and securing the confidentiality and integrity of ePHI during an emergency or disaster.

G. Evaluation.

First Transit will perform periodic technical and non-technical evaluations to assess security based initially upon the standards implemented and in response to environmental or operational changes affecting the security of ePHI .

(a) First Transit will include Security evaluations in its review of compliance with other laws.

(b) The Security Panel, or other designated person, will perform on-going reviews/evaluations to reflect all of the steps taken to comply with the Security Rule. These reviews/evaluations will be documented and maintained by the Security Panel for First Transit compliance file.

H. Business Associates and Other Contractual Arrangements

To comply with the Security Rule, First Transit will:

(a) Review current business relationships with Covered Entities and Business Associates to determine whether First Transit creates or receives ePHI in connection with the performance of a function or activity on behalf of each Covered Entity;
(b) Determine whether an addendum or modification is required to an existing agreement with a Covered Entity to address the safeguarding of ePHI;
(c) Obtain the appropriate Business Associate Agreements; and
(d) Ensure that its Business Associate Agreements are revised, when and as required to comply with HIPAA.

XXI. Physical Safeguards

Policy Statement:

It is the policy of First Transit to use physical measures, policies, and procedures designed to protect its electronic information systems and related buildings and equipment from natural hazards, environmental hazards, and unauthorized intrusion to comply with the HIPAA Security Rule.

HIPAA Requirements and First Transit Procedures:

A. Facility Access Controls

First Transit will implement policies and procedures to limit physical access to electronic information systems and the facility in which they are housed while ensuring that properly authorized Access is allowed.

1. Contingency Operations **(A)**

The Security Panel will be responsible for establishing and implementing procedures that allow access to both information systems and the facility to restore lost data and other damaged equipment in the event of an emergency.

2. Facility Security Plan **(A)**

First Transit will safeguard all of its facilities and equipment from unauthorized physical access, tampering, and theft by conducting a risk assessment, implementing a protection in depth and breadth security concept, controlling access via a secure area concept, and granting permission on an access appropriate to roll basis utilizing security systems and technologies. This may include:

(a) Providing keys to the minimum number of Workforce members that that would be practical at the given location.

(b) Prohibiting unauthorized persons, including Workforce members without clearance, Individuals, and Individual's friends and family, from physically accessing and tampering with First Transit hardware and equipment by restricting such locations as "employee only."

(c) Using and activating an appropriate theft-deterrent system or alarm.

(d) Monitoring use of access cards and keys.

(e) Deactivating lost or stolen access cards or changing locks, when necessary.

3. Access Control Procedures **(A)**

First Transit will control access to facilities based on the Workforce member's job role or function. First Transit will implement "visitor" control policies.

4. Maintenance Records **(A)**

A location manager will document all repairs and modifications to the physical components of a facility which are related to security, including any changes to hardware, walls, doors, and locks. Documentation may be kept in First Transit business records or compliance file.

B. Workstation Use (R)

Authorized Workforce shall access ePHI through First Transit Workstations solely for purposes permitted by the Business Associate Agreement, as outlined above in Section III of this Plan. Where practical, Workstations with access to ePHI ("ePHI Workstations") shall not be used by unauthorized Workforce. Location managers shall keep an inventory of all ePHI Workstations and record the location of ePHI Workstations on the inventory. If practical limit ePHI Workstations only to authorized Workforce, such Workstations shall be tagged as "Authorized Users Only." Where practical, ePHI Workstations shall be separated from other Workstations

C. Workstation Security (R)

First Transit will restrict Access to workstations to those Workforce members who are authorized users. To further promote Workstation security, Workforce members will:

(a) Comply with First Transit policy to protect an Individual's Protected Health Information from unintentional view or overheard conversations.

(b) Shield computer screens located in public areas from unauthorized viewing and/or visitors, when necessary.

(c) Control Individual, family, and visitor access to "employee only" areas of First Transit facilities.

(d) Only authorized users may log-in and access ePHI at First Transit Workstations. Users must log-out when leaving their workstations and/or protect their workstations from access by others.

D. Device and Media Controls

First Transit will implement policies and procedures that govern the receipt and removal of hardware and Electronic Media from First Transit offices and facilities. First Transit will adopt a procedure for tracking any Electronic Media containing or accessing ePHI that comes into and out of First Transit (*i.e.* information needs to be shared between First Transit's locations, offices or facilities).

1. Disposal **(R)**

First Transit will implement procedures to address the final disposition of ePHI and/or the hardware or Electronic Media on which it is stored. First Transit record disposition policy for the destruction of Individual-related and health care information (and business records) will use:

(a) A disposal destruction method which prevents any possibility of reconstructing ePHI as appropriate to the media storing the ePHI. Disposal methods include, but are not limited to:

- For paper: burning, shredding, pulping, pulverizing
- For microfilm or microfiche: recycling or pulverizing
- For laser disks in write once-read many (WORM) documents: pulverizing
- For computerized data: magnetic degaussing or overwriting (total destruction does not occur until all original and backup data are destroyed)
- For magnetic tapes: magnetic degaussing (and possibly overwriting)

(b) When necessary, First Transit will use one or more vendor(s) certified/licensed to appropriately dispose of ePHI, hardware, or Electronic Media.

(c) First Transit will document the disposal of ePHI using a form, certificate or record. Documentation will include date of destruction, method used, person(s) responsible, dates of records destroyed, a statement that the records were destroyed in the normal course of business, and signature of the supervising Individual(s).

2. Media Re-use **(R)**

First Transit will appropriately remove ePHI from electronic media before the media are made available for re-use when required by:

(a) Deleting ePHI from tapes, diskettes, rewritable CDs, and other reusable media, when necessary, using an appropriate software program.

(b) Consulting with First Transit information systems vendor to determine the appropriate removal method for the electronic media being re-used.

3. Accountability **(A)**

First Transit will maintain a record of the hardware and Electronic Media owned by First Transit and transported by Workforce members responsible for the items in a given timeframe by:

(a) Keeping an inventory and log of First Transit computers, hardware, and other Electronic Media storing ePHI.

(b) Maintaining a record of Workforce members who have access to First Transit transportable Electronic Media, such as laptops and personal electronic devices.

(c) If a laptop or other electronic device is made available or shared between workforce members, maintaining a log for signing out and returning such electronic equipment.

4. Data Backup and Storage **(A)**

First Transit will create a retrievable, exact copy of ePHI when needed, before movement of equipment by:

(a) Creating periodic backup tapes of all ePHI stored in First Transit information systems.

(b) Storing backup tapes in a secure, fireproof location.

(c) Backing up all old computers before the ePHI is deleted, if applicable.

XXII. Technical Safeguards

Policy Statement:

It is the policy of First Transit to comply with HIPAA's Security Rule by implementing policies and procedures when using technology to protect ePHI and to control Access to it.

HIPAA Requirements and First Transit Procedures:

A. Access Control

First Transit will implement technical policies and procedures for its electronic information and computer systems to maintain ePHI and to allow Access to only those Workforce members who have been granted Access rights.

1. Unique User Identification **(R)**

If practicable, each Workforce member with access to ePHI will be assigned a unique name and/or number for identifying and tracking user identity. The Security Panel or designee will assign and track the unique user identification according to First Transit employee and security policies.

2. Emergency Access Procedure **(R)**

First Transit will use, as needed, the following procedures for obtaining necessary ePHI during an emergency:

(a) The Security Panel and Compliance Officer will determine the necessary amount of ePHI requiring access during an emergency.

(b) Senior management will determine whether backup tapes should be obtained from storage.

(c) The Security Panel and Compliance Officer may consult with one or more vendors to determine what, if any, additional actions to take in the event of an emergency.

3. Encryption and Decryption **(A)**

If required, reasonable, and attainable, First Transit will implement a mechanism to encrypt and decrypt stored ePHI. First Transit will assess whether this Security measure is reasonable during the periodic evaluations required by the security policies.

4. Automatic Logoff **(A)**

If reasonable and appropriate for First Transit operations, and to implement additional security measures without jeopardizing the integrity and confidentiality of ePHI, First Transit will:

(a) Develop and use a method for terminating an electronic session (*i.e.* computer access) after a predetermined time of inactivity.

(b) Assess additional Security measures are required during the periodic evaluations required by the Security policies.

B. Audit Controls (R)

When reasonable and practicable, First Transit will use any and all hardware, software, and/or procedural mechanisms that record and examine activity in its information systems that contain or use ePHI. The Security Panel or designee will audit such information at regular intervals. First Transit will assess whether this Security measure is reasonable during the periodic evaluations required by the Security policies.

C. Integrity (A)

First Transit will protect ePHI from improper alteration or destruction. First Transit will determine reasonable methods for authenticating ePHI. First Transit may use one or more external vendors.

D. Person or Entity Authentication (R)

If practicable, First Transit will verify that a person or entity seeking Access to ePHI is the one claimed through the use of unique user IDs and passwords.

E. Transmission Security

First Transit will use appropriate and reasonable technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communication network.

1. Integrity Controls **(A)**

First Transit will comply with applicable industry best practices transmitting billing data and other Individual information to ensure the Integrity and Security of transmitted ePHI, when applicable.

2. Encryption **(A)**

First Transit will comply with applicable industry best practices for transmitting billing data to ensure the Integrity and Security of transmitted ePHI.

XXIII. Breach Notification

Policy Statement:

It is the policy of First Transit to comply with the provisions contained in HIPAA regarding notification in the case of a Security Breach.

HIPAA Requirement and First Transit Procedure:

In case of Security Incident, First Transit will immediately perform a Breach analysis and consider all of the following:

- Nature of Protected Health Information
- Who
- Evidence of Access or Disclosure
- Mitigation of Risk

First Transit shall, upon discovery of a Breach of Unsecured Protected Health Information, notify the Covered Entity promptly. Such notice will be given as soon as possible in accordance with the provisions set forth below.

- Breaches Treated as Discovered: A Breach shall be treated as discovered by First Transit as of the first day on which such Breach is known to have occurred (including any person, other than the person committing the Breach that is an employee, officer or agent of the entity or associate) or should reasonably have been known to such entity or associate to have occurred.

- Timing of Notification: All required notifications shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach by First Transit unless delayed notice is required for law enforcement purposes. First Transit shall maintain a copy of the notice (whether sent in paper or electronic form) to the appropriate Covered Entity of Business Associate.

- Methods of Notice: Notice shall be sent in paper or electronic form to the Covered Entity by the Compliance Officer (or his/her designee). The Compliance Officer shall maintain a copy of such notice in the compliance file. Unless otherwise required by HIPAA or under the terms of a Business Associate Agreement between First Transit and the Covered Entity or Business Associate affected by the Breach of Unsecured Protected Health Information, First Transit shall not provide notice of Breach to any Individual or the Secretary of Health and Human Services.

  Content of Notification: First Transit shall provide notice that includes, to the extent possible, the identification of each individual whose unsecured PHI has been

or reasonable believed by First Transit to have been accessed, acquired, used or disclosed during the breach

If available, First Transit shall provide the following at the time of notification of promptly thereafter as the information becomes available

1. a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
2. 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, or disability code);
3. the steps Individuals should take to protect themselves from potential harm resulting from the Breach;
4. a brief description of what First Transit is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches; and
5. contact procedures for Individuals to ask questions or learn additional information, which will include a toll-free telephone number, an email address, website or postal address.

XXIV. Security Rule Documentation

Policy Statement:

It is the policy of First Transit to comply with the HIPAA Security Rule's requirements for documentation of compliance actions.

HIPAA Requirement and First Transit Procedure:

First Transit will document all steps and actions taken to comply with the HIPAA Security Rule. Documentation will include:

- Risk analyses and assessments, including evaluation of whether an addressable implementation specification applies to First Transit.
- Security Incident Reports
- Audit Reports
- Business Associate Agreements
- Disposal/destruction of Electronic Media
- Records related to information system updates, Security modifications, software or hardware changes, etc.
- Workforce training and updates on Security
- All other records relating to steps taken by First Transit to comply with the Security Rule

Documentation will be maintained by the Security Panel or in First Transit HIPAA compliance file and will be available to persons responsible for implementing First Transit Security measures and policies. Documentation will be reviewed by the Security Panel periodically and updated as needed, in response to operational, environmental, personnel, or administrative changes affecting the security of ePHI.

XXV. Duty of Workforce Members to Report Security Breaches

Policy Statement:

It is the policy of First Transit to maintain compliance with the HIPAA Security Rule and require Workforce members to report all known or suspected security incidents and Breaches to the Security Panel.

First Transit Policy:

This duty to report requires all Workforce members who require access to e-PHI to perform job duties to report any concerns they may have about the Security of Individuals' health information that is created or stored electronically to the Security Panel.

Workforce members should:

- Report any unauthorized persons Accessing First Transit computers and electronic media.

- Not download or upload any unapproved software or files sent by e-mail without permission from the Security Panel.

- Be aware of Workforce, Individuals, visitors, and all other persons who are present in First Transit offices, at all times.

Workforce members are expected to be familiar with and abide by First Group's Acceptable Use Policy

FORMS
HIPAA Forms

Form No. 1: Concern or Complaint Form
Form No. 2: Complaint Record and Disposition
Form No. 3: Security Incident Report
Form No. 4: Workforce Training Certificate & Confidentiality Agreement

FORM NO. 1: Concern or Complaint Form

FIRST TRANSIT, INC.
CONFIDENTIAL QUESTION OR COMPLAINT FORM

Please let us know immediately if you have a question, concern, or complaint about First Transit practices regarding the privacy of Protected Health Information or Electronic Protected Health Information.

Please complete this form, mark the envelope "Confidential" and send it to the attention of the Compliance Officer, First Transit. 600 Vine Street, Suite 1400, Cincinnati, OH 45205.

If you prefer to discuss your questions, concerns or complaint, please contact our hotline at 1-877- 3CallFG and request a call back from our Compliance Officer regarding a HIPAA issue. You may also contact the Compliance Officer via e-mail at hotline@FirstGroup.com, attn: HIPAA Compliance Officer.

What is your privacy question, concern, or complaint?

_____

_____

_____

If you believe your privacy rights have been violated, when do you believe this violation occurred? _____

_____

Is there a particular person who you believe violated your privacy rights? If so, please identify, either by name or by job description: _____

_____

It is not necessary for you to give us your name, telephone number or address. However, we encourage you to include this information, so we may give you an answer or give you direct feedback in resolving your concern or complaint. We appreciate your bringing any problems to our attention and will never "retaliate" against you for expressing a concern or complaint.

_____

Name

_____

Address Telephone

We promise to address all questions and investigate all concerns and complaints promptly.

Do you prefer for us to send you a written response or call you? _____
Please provide address and/or phone number below.

_____

_____

_____

We believe in the confidentiality and proper Use and Disclosure of health information.

We pledge to resolve concerns and complaints to your satisfaction.
Thank you for your cooperation.

FORM NO. 2: Complaint Record and Disposition

COMPLAINT RECORD AND DISPOSITION
TO BE COMPLETED BY COMPLIANCE OFFICER

Date Complaint Received: _____

Nature of the question, concern or complaint _____
_____
_____
_____

Date when violation allegedly occurred _____

Person(s) who allegedly violated the Individual's privacy rights _____
_____
_____

Investigation steps, including documents reviewed and persons interviewed _____
_____
_____
_____
_____

Disposition: Violation _____ No violation_____

If violation, Corrective Action or Discipline taken _____
_____
_____
_____
_____
_____

Should First Transit privacy practices be revised to prevent the same or similar recurrences?
Yes____ No_____

Feedback to Individual/Individual: Date_____ Written _____ Oral _____

Did the Individual/Individual appear satisfied? Yes _____ No _____

Signature of person completing this form: _____

FORM NO. 3: Security Incident Report

SECURITY INCIDENT REPORT FORM

Date:_____ Location:_____

*Name:_____ *Position:_____

*Phone Number:_____ *Supervisor:_____

Incident
Description of incident (including number of patients affected):_____

_____

_____

_____

_____

The following is to be completed by Security Panel or his/her designee.
Is this incident likely to compromise the privacy or security of the PHI at issue? _____

Date reviewed by Security Panel:_____

Action taken:_____

_____

_____

_____

Follow-up:_____

_____

_____

_____

_____

FORM NO. 4: Workforce Training Certificate & Confidentiality Agreement

FIRST TRANSIT, INC.
HIPAA AWARENESS TRAINING CERTIFICATION
& CONFIDENTIALITY AGREEMENT

Today I completed HIPAA awareness training and Security training that included: (1) an overview of the basic terms and operation of HIPAA's privacy and security standards concerning the use and disclosure of Protected Health Information ("PHI") and safeguarding PHI and Electronic Protected Health Information ("e-PHI"); (2) a review of the First Transit policies and practices regarding the privacy and security of PHI and e-PHI; and (3) the First Transit Complaint Procedure.

I understand that I may have been granted access to PHI and e-PHI for the sole purpose of performing my job duties as a member of First Transit workforce. I understand that maintaining the confidentiality of this information and using and disclosing this information properly is a requirement of my job. I understand that, as a member of First Transit workforce, I share in the responsibility to assist First Transit in compliance with the privacy and security standards under HIPAA. I promise to take reasonable steps in performing my job duties to safeguard the privacy and security of our PHI and e-PHI, and I will limit my access to this information to the "minimum necessary" for me to perform my job duties and responsibilities.

I will report my concerns about suspected violations, privacy breaches, security incidents, and breaches of Unsecured Protected Health Information to the Compliance Officer or the Security Panel immediately so that corrective action can be taken. I may contact these parties via email at HIPAA@Firstgroup.com Attn: Compliance Officer or Security Panel, or by calling First Transit's hotline at 1-877-3CallFG.

I understand that the duty to respect and maintain the privacy and security of PHI and e-PHI is ongoing and does not end if I voluntarily or involuntarily leave First Transit workforce. If I leave First Transit, regardless of reason, I agree not take with me originals or copies of PHI or e-PHI and to return or destroy any PHI or e-PHI in my possession.

Upon my leaving the First Transit, I agree to return any confidential and proprietary information belonging to the First Transit, including (without limitation) Individual lists and demographic information, billing information, financial information, contract and strategic planning information. I promise not to Disclose this confidential and proprietary information to any unauthorized person or competitor of the First Transit, and I promise not to use it to the detriment of the First Transit.

_____
Print Name

_____ _____
Signature Date

APPENDIX OF SELECT RESOURCES: TABLE OF CONTENTS

1. Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 (Subpart E, together with the definitions in Subpart A).

2. Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164 (Subpart C, together with the definitions in Subpart A).

3. Health Information Technology for Economic and Clinical Health Act (HITECH), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (2009).

4. Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Parts 160 and 164 (Subpart D).