POLICY:

This policy reflects the continued commitment of Chatham Area Transit Authority to protect the confidentiality of its Plan participants' protected health information ("PHI") held by the Authority's employee Health Plans (the "Plan") under the Health Information Portability and Accountability Act (HIPAA).

Chatham Area Transit Authority's Health Plan Providers, Third Party Administrators and other Business Associates, that assist in the administration of the Plan, are covered under business associate agreements requiring confidentiality of the Authority's Plan participants' PHI.

I. Definitions

Breach means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term "breach" does not include the following:

1. Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if:

   a. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and

   b. Such information is not further acquired, accessed, used, or disclosed by any person.

2. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at same facility;

3. Any such information received as a result of disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

HR staff means personnel providing administration duties whom have access to enrollment, eligibility and contribution data of individual enrollees in the Authority's Health Plan. This list includes but is not limited to Human Resources, Payroll Personnel, Department Managers, and the CEO.

Privacy Official means the person designated to implement enforce and administer HIPAA compliance efforts in regards to Chatham Area Transit's Health Plan. The Privacy Official can be contacted by mail at Attn: Human Resources, Chatham Area Transit Authority, 900 E. Gwinnett St., Savannah, GA 31401or by phone at 912-629-3906.

Protected health information (PHI) means any information that may identify Plan participants and that relates to health care services provided to Plan participants, the payment of health care services provided to Plan participants, or Plan participants' physical or mental condition, in the past, present and future. Also included as PHI is any information connected to enrollment, eligibility, or contribution amounts made to an Flexible Spending Account (FSA).

II. PHI Uses and Disclosures

All uses and disclosures of PHI shall be in accordance with the Plan's HIPAA Notice of Privacy Practices and this policy and its corresponding procedures.

The Plan may use and disclose Plan participants' PHI, without authorization, for the following purposes:

- Treatment, payment and health care operations;
- Administrative functions of the Plan;
- Communications with the enrollee or their designated representative, health care providers, third party administrators, and other business associates;
- Research (subject to strict legal restrictions);
- Compliance with Workers' compensation programs, government agencies, court proceedings, law enforcement activities, and public health activities.
- HR staff may internally use or externally disclose PHI in the following circumstances:
- To enter, update, or use enrollment, eligibility, and payroll deduction information in ADP and in vendor enrollment websites;
- Pursuant to requests by an enrolled employee or an employee's personal representative;
- Pursuant to a valid court order, subpoena or warrant;
- When authorized by the enrollee using the appropriate HIPAA Disclosure Authorization Form;
- When authorized by the Privacy Official.

When collecting or receiving PHI, HR staff will request only the minimum necessary information to carry out administrative functions of the Plan. Any documentation supporting the authority to disclose PHI to parties other than HR staff and the Corporate Benefits Department must be retained in the employee's Benefit/HIPAA Folder for up to six (6) years after separation.

Any doubts regarding the appropriateness of a use or disclosure must be directed to the Privacy Official for clarification.

HR staff shall promptly report any known unauthorized uses or disclosures of PHI to the Privacy Official.

III. Plan Participant Rights in Relation to PHI

HR staff shall recognize and respect the following Plan participants' HIPAA Medical Privacy rights in relation to PHI.

Right to Request Restrictions
Plan participants may request that the Plan limit the uses and disclosures of their PHI regarding treatment, payment and health care operations; and/or on the use and disclosure of PHI to a family member or close friend that is involved in the participant's care. The participant may also request not to use or disclose PHI at all. The Access, Amend or Restrict Form must be completed and forwarded to the Privacy Official. While reasonable requests may be accommodated, agreement to a requested restriction is not required unless the request is for non-disclosure regards a specific health care item or service for purposes of payment; or for health care operations that have been paid for in full out of pocket by the Plan participant. The Privacy Official will respond directly to the participant's restriction request.

Right to Receive Confidential Communications
Plan participants may request to receive their confidential information from the Plan at an alternative location or by an alternative means of communication. All requests must be in righting and forwarded to the Privacy Official. While reasonable requests may be accommodated, agreement to a request is not required. The Privacy Official will respond directly to the participant's request.

Right to Access PHI
Plan participants have the right to inspect and copy their PHI that the Plan maintains. A Plan participant may request an electronic copy of their health information if it is maintained in an electronic health record. A Plan participant may also request that such electronic health information be sent to another entity or person, so long as that request is clear, conspicuous and specific. The participant may be charged for the cost of copying and mailing, if applicable. The requested information will generally be provided within 30 days if the information is maintained within a Chatham Area Transit Authority location. Information kept off site or with a Health Care Provider may take longer.

The Access, Amend or Restrict Form must be completed and forwarded to the Privacy Official prior to release of any PHI. Denial of a request may be made in certain instances as defined by law. The Privacy Official will respond directly to the participant's request.

Right to Receive a Copy of the HIPAA Notice of Privacy Practices
Plan participants have the right to request a paper copy of the HIPAA Notice of Privacy Practices. All requests must be made in writing and forwarded to the Privacy Official. The Privacy Official will respond directly to the participant's request.

Right to Amend PHI
Plan participants have the right to request that the Plan amend their PHI. The Amend,

Access or Restrict Form must be completed and forwarded to the Privacy Official. Denial of a request may be made if the PHI is accurate and complete, was not created by the Plan, or is not available for inspection as defined by law. The Privacy Official will respond directly to the participant's request.

Right to Receive an Accounting of Disclosures

Plan participants have the right to receive a list of the Plan's disclosures of their PHI, except for those disclosures that are made in connection with claims payment, treatment, healthcare operations or disclosures authorized by the participant, and certain other disclosures unless those disclosures involve an electronic record of health-related information on the individual that is created, gathered, managed or consulted by authorized health care staff. The accounting covers up to 6 years prior to the request, except in regards to electronic records where the accounting need only date back 3 years. All requests must be made in writing and forwarded to the Human Resources Department. Participants may request one (1) accounting in a twelve (12) month period free of charge. Participants may be charged for subsequent requests within the twelve (12) month period. The Privacy Official will respond directly to the participant's request.

Right to File a Complaint

Plan participants have the right to file a complaint if they believe their HIPAA Medical Privacy rights have been violated. Plan participants may file a written complaint with the Privacy Official by completing a HIPAA Privacy Complaint Form. A participant may also file a complaint with the Secretary of the Department of Health and Human Services. The Privacy Official will respond directly to the participant's complaint appropriately.

It is the policy of the Authority to comply with its legal obligations regarding Plan Participant's PHI. It is also the policy of the Authority to prohibit any intimidation, threats, coercion, discrimination or other retaliatory acts against any person for exercising his or her rights under HIPAA or any other applicable law.

IV. Safeguarding Protected Health Information

Chatham Area Transit Authority is committed to safeguarding plan participants' PHI and, as such, must take reasonable steps to ensure that PHI is not intentionally or unintentionally used or disclosed in any manner not consistent with HIPAA Medical Privacy Regulations. HR staff must comply with the following HIPAA Medical Privacy procedures below, along with any additional or updated guidelines as established by the Human Resources Department:

1. When HR staff are actively using PHI during work hours, they must:
   - Maintain all hard copy PHI in a concealed folder or binder;
   - Password protect electronic PHI, especially when sending via e-mail;
   - Utilize computers screen saver function;
   - Position computer monitor screen away from common areas and office doors that

are utilized by employees-at-large or the general public.

2. When HR staff must leave their work space during work hours, they must:
   • Make sure PHI data is secure by either placing documents in locked file cabinets and/or locked desk drawers or by locking their office door (if applicable);
   • Close out of software programs, making sure all electronic PHI is password protected.

3. When HR staff leave work for the day, they must:
• Close out of all software programs, log completely off, and shut down computer;
• Make sure all file cabinets and desk drawers containing PHI are securely locked;
• Lock office door (if applicable).
4. Hard copy and electronic documents containing PHI should have all information that identifies or could reasonably be used to identify an individual deleted or removed wherever possible.
5. Once documents containing PHI no longer need to be retained after use, unless subject to HIPAA Privacy Retention Requirements, they must be destroyed (i.e., shred hard copy, delete file from computer).

V. Breach Notification Rules

The Plan has an obligation to notify certain parties of any "breach" of PHI, i.e., the "unauthorized acquisition, access or use of disclosure of unsecured PHI which compromises the security or privacy of such information." Unsecured PHI is any PHI that has not been encrypted or destroyed. PHI that is secured is not subject to breach rules.

Determination if a Breach has occurred. The following approach will be followed to determine if a breach has occurred:

1. Determine whether there has been an impermissible use or disclosure of PHI under the HIPAA Medical Privacy and Security Rules;

2. Determine whether such impermissible use or disclosure compromises the security or privacy of the PHI-that is, if it poses a significant risk of financial, reputational, or other harm to the individual-and document the risk assessment performed in making this determination; and

3. Determine whether the incident falls within one of the three limited exceptions to the definition of "breach." For example, an unintentional disclosure of PHI by someone authorized to access PHI to another authorized individual, if done in good faith and within the person's scope of authority but does not result in further impermissible use or disclosure of the PHI would not be a "breach."

Required Notifications. If the Plan determines that a breach has occurred, the Plan will take

the following notification steps:

1. *Notification to Individuals.* Written notice to affected individuals must generally be given by first class mail. The notice must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. The notice must be provided by the Plan "without unreasonable delay" – but in no case later than 60 days after discovery of a breach of unsecured PHI.

2. *Notification to Media.* If the PHI of 500 or more individuals in a single State or jurisdiction is involved in the breach, notice must be given to prominent local media outlets within the same timeframe stated in (1.) above.

3. *Notification to Health & Human Services (HHS).* If the PHI of 500 or more individuals is involved in the breach, HHS must be notified at the same time as individual notice is provided. If the PHI of less than 500 individuals is involved in the breach, the Plan must maintain a log and submit it annually to HHS (within 60 days after the end of the calendar year).

VI. PHI Retention

A Benefit/HIPAA Folder must be kept separately or with the medical personnel file of each employee that contains all documents related to enrollment and eligibility in the Authority's Plans. Copies of files or documents must be retained for at least six (6) years after separation of the employee. The file contents may include:

- Enrollment forms, including supporting documents such as birth certificates;
- Enrollee use and disclosure authorization forms;
- Employee requests to exercise HIPAA rights (although original should be sent to Privacy Official);
- Documents supporting disclosures to personal representatives and government officials;

Other documents related to the Authority's Health Plans that the Human Resources Department requests be included.

APPLIES TO:

All employees of Chatham Area Transit Authority.