PA TURNPIKE COMMISSION POLICY *This is a statement of official Pennsylvania Turnpike Policy*		**NUMBER**: 2.11 **APPROVAL DATE**: 04-15-2003
POLICY SUBJECT: Health Insurance Portability and Accountability Act (HIPPA)	**RESPONSIBLE DEPARTMENT:** Human Resources	**EFFECTIVE DATE**: 04-15-2003 **REVISED DATE**: 04-02-2003

A. PURPOSE:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required regulations to implement a comprehensive federal law to protect individually identifiable healthcare information. The Privacy Rule creates national standards to protect medical records and other protected health information (PHI).

This policy governs the efforts of the Pennsylvania Turnpike Commission to comply with the relevant provisions of the Health Insurance Portability and Accountability Act (HIPAA). Procedures are included that outline privacy, use and disclosure of protected health information (PHI).

B. SCOPE:

This policy applies to all employees and all business associates including, but not limited to, contractors, consultants and vendors, of the Pennsylvania Turnpike Commission.

C. GENERAL POLICY:

The Commission's policy is to:

- Provide security of protected health information.
- Use PHI only as necessary. Some examples of use are:
  - To communicate with health care professionals who care for you
  - To obtain reimbursement from private insurers
  - To verify that services billed were actually provided
  - To assess and improve the services provided and the outcomes achieved
  - To pay for services you receive
  - To inform you about other public programs and services
- Disclose PHI to our business associates when it is necessary.
- Ensure compliance with HIPAA.

D. DEFINITIONS:

Business Associate- A person or entity who, on behalf of a covered entity or an organized health care arrangement, performs or assists in the performance of:

1. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, utilization review, quality assurance, billing benefit management, practice management, and re-pricing; or

2. Provides legal, actuarial accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for such covered entity or organized health care arrangement

Business Associate Agreement- A contract between a covered entity and a business associate that must:

1. Establish the permitted and required uses and disclosures of personal health information (PHI) by the business associate.

2. Provide that the business associate will use PHI only as permitted by the contract or required by law, use appropriate safeguards, report any disclosures not permitted by the contract, ensure that only agents to whom it provides PHI will abide by the same restrictions and conditions, make PHI available to individuals, make its records available to Health and Human Services; and

3. Authorize termination of the contract by the PTC if the PTC determines that there has been a violation of the contract.

The Business Associate Agreement is usually part of a contract made in the procurement process but can be part of a Memorandum of Understanding, Grant Agreement or other documents.

Covered Entity- A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction. The PTC is a covered entity as a health plan since it is self-insured.

Disclosure- Releasing, transferring, providing access to, or divulging in any other manner, information outside the entity holding the information.

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

Health Information- Any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. Relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual.

Individual- The person who is the subject of protected health information.

Individually Identifiable Health Information- Health information, including demographic information collected from an individual that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI)- Individually identifiable health information that is transmitted by electronic media, maintained in any medium, transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act.

Privacy/Client Information Officer- To ensure compliance, the Privacy Rule requires that covered entities designate a Privacy Officer who is responsible for the development and implementation of privacy policies and procedures. The Privacy Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the PTC's policies and procedures covering the use, and access to, protected health information in compliance with federal and state laws. The PTC Privacy Officer is the Manager of Compensation and Benefits, Human Resources Department. The role of the Privacy Officer is to:

1. Provide guidance and assist in the identification, implementation, and maintenance of information on privacy policies and procedures.

2. Perform initial and periodic information privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with the Commission's other compliance and operational assessment functions.

3. Work with individual departments to ensure that the Commission has and maintains appropriate privacy consent and authorization forms, information notices and materials reflecting current policies and procedures.

4. Oversee delivery of initial privacy training to all Commission employees.

5. Oversee delivery of initial guidance to contractors, business associates, and other appropriate third parties.

6. Participate in the development of all trading partner, chain of trust and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.

7. Establish and administer a process for receiving, documenting, tracking, investigating, and taking action when appropriate, on all complaints concerning the Commission's privacy policies and procedures in coordination with other similar functions and, when necessary, the Legal Department.

8. Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the Commission's workforce.

9. Work with all Commission personnel involved with any aspect of release of protected health information to ensure full coordination and cooperation under the Commission's policies and procedures.

10. Monitor changes in applicable federal and state privacy laws and advancement in information privacy technologies to ensure PTC compliance.

11. Cooperate with the Department of Justice, Office for Civil Rights, PTC auditors and legal staff in any appropriate compliance review or investigation.

Privacy Rule-The Privacy Rule, as published in the Code of Federal Regulations, creates national standards to protect medical records and other protected health information (PHI). The Privacy Rule sets a minimum standard of safeguards of PHI and requires the PTC to take certain actions, such as the actions outlined in this policy.

Use- With respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.

E. PROCEDURES:

Minimum Necessary Standard. The PTC must restrict access and use of PHI to the minimum necessary for an employee to perform their specific job function. Electronic and manual access to PHI will be determined by the scope and responsibilities of an employee's position. Specific access must be listed in all departments' policies and job descriptions, as appropriate.

Routine disclosures must always be limited to the minimum necessary to meet the purpose of the disclosure. For example, a minimum disclosure for oversight purposes could include large numbers of records with minimal identifying information in order to identify treatment or payment patterns.

Business Associates. 45 CFR § 164.502(e)(1) requires that in order to disclose PHI to a business associate, a program office must receive satisfactory assurance that the business associate will appropriately safeguard the information. Under the Privacy Rule, satisfactory assurances must be obtained in a contract or other written arrangement. The Legal Department has developed Business Associate Language that all departments must adapt to fit their and their business partners needs. (See Appendix A).

The individual departments, in conjunction with the Contracts Administration Department, will review relationships with business partners to determine whether it is appropriate to execute a business associate agreement.

Security of Personal Health Information (PHI). The PTC will ensure all PHI is properly secured at all times. Written PHI will be secured at work locations in locked drawers and file cabinets. Electronic PHI will be password protected and secured. PHI will only be provided to individuals when necessary. Individuals granted access to PHI will be instructed to maintain confidentiality of the information and ensure proper use of the information.

Use and Disclosure of PHI. Use of PHI will be limited to those individuals involved in the operation and administration of employee benefit programs. PHI will only be disclosed to outside business associates when necessary. Some examples of use are: to communicate with health care professionals who care for you; to obtain reimbursement from private insurers; to verify that services billed were actually provided; to assess and improve the services provided and the outcomes achieved; to pay for services you receive; and, to inform you about other public programs and services. Any other use or disclosure requires authorization by the employee.

Restriction on Uses and Disclosures. Individual employees have the right to request restrictions on the use and disclosure of his/her protected health information. If the requested restrictions are within the scope of the law, the PTC would not use or disclose PHI that is inconsistent with the restrictions, unless mandated by law to do so.

Privacy Officer. The Commission has designated the Manager of Compensation and Benefits, Human Resources Department as the HIPAA Privacy Officer. An overview of the duties and responsibilities of the Privacy Officer are outlined in the definition section of this policy. Any questions, concerns or complaints regarding compliance with HIPAA should be directed to the Privacy Officer.

Employee Training. All employees will receive training on the HIPAA policies and procedures. Training will be tailored to the requirements necessary to enable the employee to carry out their job responsibilities. The level of training will depend upon the employee's contact with or access to PHI.

Rights of Employees. HIPAA gives an individual the right to access, inspect and obtain a copy of PHI. Employees also have the right to:

- Request a restriction on certain uses and disclosures of their protected health information.
- Request amendments to their protected health information.
- Obtain an accounting of disclosures of their protected health information.
- Request that their protected health information be communicated by an alternative means or to an alternative address or to an alternative individual.
- Revoke their consent to use or disclose protected health information to the extent that it has not already been relied upon.
- File a complaint to the Privacy Officer and/or the Secretary of the U. S. Department of Health and Human Services if they believe their privacy rights have been violated.

The Human Resources Department will establish procedures to address individual requests.

Violations. All employees are required to comply with the provisions of this policy letter. Employees found to be in violation of this policy will be subject to disciplinary action, up to and including dismissal.

Business Associate Agreements. The PTC may enter into a contractual relationship with a business associate that may involve disclosure of PHI. When this occurs, our contract with the

outside organization will include a business associate agreement (see Appendix A). This agreement requires the outside organization to comply with the provisions of HIPAA. The Contracts Administration Department will work with program managers to ensure the appropriate business associate agreements are established.

The Privacy Officer and Human Resources Department may develop additional procedures to ensure PTC business practices comply with HIPAA.

This Policy Letter supersedes all previous Policy Letters on this subject.