PENNA TURN PIKE	**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**: 12-19-2023

A. PURPOSE:

The Pennsylvania Turnpike Commission (Commission) provides employee health benefits through the Commission's Employee Group Benefit Plan(s) ("Plan"). The Commission adopts this policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations on protecting the privacy and confidentiality (the "Privacy Standards") of the Plan Members.

B. SCOPE:

This policy letter applies to all employees and Business Associates of the Commission.

C. GENERAL POLICY:

The Commission protects the privacy and confidentiality of Protected Health Information (PHI) whenever it is used by Commission representatives. The private and confidential use of such information will be the responsibility of all employees and Business Associates with job duties requiring access to PHI in the course of their jobs.

As a Covered Entity the Use of PHI will be limited to those employees and/or Business Associates involved in the operation and administration of employee benefit programs. PHI will only be Disclosed to outside Business Associates when necessary. The Commission is required by law to maintain the privacy of PHI and any other Use or Disclosure requires written authorization by the Individual.

Individuals have the right to:

- Access, inspect and obtain a copy of PHI.
- Request a restriction on certain Uses and Disclosures of their PHI.
- Request amendments to their PHI.
- Obtain an accounting of Disclosures of their PHI.
- Request that their PHI be communicated by an alternative means or to an alternative address or to an alternative Individual.
- Revoke their consent to Use or Disclose PHI 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 Commission has designated the Program Manager of Benefits and Retirement in Human Resources (HR) as the HIPAA Privacy Officer. Any questions, concerns, or complaints regarding compliance with HIPAA should be directed to the Privacy Officer.

D. DEFINITIONS:

Business Associate – In accordance with this policy a business associate is 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 but not limited to claims processing or administration, utilization review, quality assurance, maintaining or transmission of data, 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 (BAA) **–** A HIPAA Business Associate Agreement is a required contract between a Covered Entity and a Business Associate providing written, contractual assurance that the business associate will maintain a specific set of standards for the protection of PHI. BAAs are most often included as part of a contract with a Business Associate.

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 Commission's self-inured group health plans are considered a Covered Entity.

Disclosure **–** The releasing, transferring, providing access to, or divulging in any other manner of information outside the entity holding the information.

Electronic PHI (ePHI) – Any PHI that is created, stored, transmitted, or received in any electronic format or media. ePHI includes distinct demographics that can be used to identify a patient.

Health Care Provider **-** A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business and who transmits any Health Information in electronic form in connection with PHI.

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

- 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

- Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an individual; or past, present, or future payment for the provision of health care to an individual.

Individual **-** The person who is the subject of PHI.

Individually Identifiable Health Information (IIHI) **-** Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of IIHI include, but are not limited to:

- Name: full name, maiden name, mother's maiden name, or alias
- Personal identification numbers: social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number
- Personal address information: street address, or email address
- Personal telephone numbers
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting
- Biometric data: retina scans, voice signatures, or facial geometry
- Information identifying personally owned property: VIN number or title number
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person

Privacy Officer **-** The employee responsible for the development, implementation, maintenance of and adherence to the Commission's policies and procedures covering the use, and access to, PHI in compliance with federal and state laws.

Protected Health Information (PHI) - IIHI received by a Covered Entity that relates to the past, present, or future health of an Individual or to payment of health care claims. PHI includes medical conditions, health status, claims experience, medical histories, physical examinations, genetic information, and evidence of disability. PHI does not include Health Information held by the Commission in its role as an employer, such as information collected from an employee or an employee's health care provider to support an employee's request for Family and Medical Leave Act leave, to verify Americans with Disability Act status, workers' compensation claims processing, for payment of an invoice or information received for education records.

Use **-** The sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information.

E. PROCEDURES:

Each department is responsible to ensure access, use, and disclosure of PHI and IIHI is restricted to the minimum necessary for an employee to perform their specific job function. Routine disclosures must always be limited to the minimum necessary to meet the purpose

of the Disclosure. Written PHI and IIHI should always be forwarded to the Human Resources (HR). Until this information can be forwarded to HR it must be secured at work locations in locked drawers and file cabinets. ePHI shall be password protected and secured.

Employees and Business Associates granted access to PHI are required to maintain confidentiality of the information, ensure proper use of the information, and comply with the Commission's 8.01 Acceptable Use of Commission Technology Resources and 8.07 Mobile Device policy letters.

BAAs will be included as part of the contract with Covered Entities to ensure protection of ePHI.

Employees are required to take 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.

In the event of a breach of unsecured PHI, HR must be notified immediately. The Commission and/or its Business Associate(s) shall provide any required notifications in accordance with the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

Employees and Business Associates are directly liable under the HIPAA Rules and may be subject to civil and, in some cases, criminal penalties for uses and disclosures of PHI that are unauthorized or not otherwise required by law.

All employees and Business Associates are required to comply with the provisions of this policy letter. Employees or Business Associates found to be in violation of this policy will be subject to disciplinary action, up to and including termination of employment, contract, or agreement.

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