May 9, 2005

HIPAA SECURITY COMPLIANCE GUIDE©

FOR

PIONEER EDUCATORS HEALTH TRUST

.

Revised 9-2008

PIONEER EDUCATORS HEALTH TRUST
HIPAA Security

Introduction

Various sponsoring employers (referred to collectively as the "Company") sponsor a multiple employer welfare arrangement entitled the PIONEER EDUCATORS HEALTH TRUST (the "Plan"). Members of the Company's workforce may create, receive, maintain, or transmit electronic protected health information (as defined below) on behalf of the Company, for Plan administration functions.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations require the Plan to implement various security measures with respect to electronic protected health information (electronic PHI).

> *Electronic Protected Health Information* is protected health information that is transmitted by or maintained in electronic media.
>
> *Protected Health Information* (PHI) is the information that is subject to and defined in the Plan's privacy policies and procedures.
>
> *Electronic Media* means:
>
> 1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
>
> 2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

It is the Plan's policy to comply fully with HIPAA's requirements.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan. This Policy does not address requirements under federal laws other than HIPAA or under state laws.

I. Security Officer

Keith Grimm is the Security Officer for the Plan. The Security Officer is responsible for the development and implementation of the Plan's policies and procedures relating to security, including but not limited to this Policy.

II. Risk Analysis

The Plan has no employees. All of the Plan's functions, including creation and maintenance of its records, are carried out by employees of the Company. (For purposes of this Policy, the term "employee" includes individuals such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company.) The Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Company. Accordingly, the Company creates and maintains all of the electronic PHI relating to the Plan, owns or controls all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and controls its employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Plan has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Plan. That ability lies solely with the Company.

Because the Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Company affecting the security of Plan electronic PHI, and the Company has undertaken certain obligations relating to the security of electronic PHI that it handle in relation to the performance of administration functions for the Plan, the Plan's policies, and procedures, including this Policy, do not address the following standards (including the implementation specifications associated with them) established under HIPAA and are set out in Subpart C of 45 CFR Part 164:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and

- transmission security.

III. Plan Document

The Plan document shall include provisions requiring the Company to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Company creates, receives, maintains, or transmits on behalf of the Plan (the Plan electronic PHI);

- ensure that reasonable and appropriate security measures support the Plan document provisions providing for adequate separation between the Plan and the Company (which were adopted as described in the plan's privacy policy);

- ensure that any agents or subcontractors to whom the Company provides Plan electronic PHI agree to implement reasonable and appropriate security measures to protect the Plan electronic PHI; and

- report to the Security Officer any security incident of which the Company becomes aware.

IV. Disclosures of Electronic PHI to Business Associates

A business associate is an entity (other than the Company) that:

- performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or

- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

In the future, the Plan may permit one or more business associates to create, receive, maintain, or transmit electronic PHI on its behalf only if the Plan first obtains satisfactory assurances from the business associate that it will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract providing that the business associate will:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the Plan (the Contract electronic PHI);

- ensure that any agents or subcontractors to whom the business associate provides Contract electronic PHI agree to implement reasonable and appropriate security measures to protect the Contract electronic PHI;

- report to the Plan any security incident of which the business associate becomes aware; and

- authorize termination of the contract by the Plan if the Plan determines that the business associate has violated a material term of the contract.

V. Documentation

The Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Plan electronic PHI, and any changes to policies or procedures will be documented promptly.

Except to the extent that they are carried out by the Company or business associates, the Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the Plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Plan will make its policies, procedures, and other documentation available to the Security Officer and the Company, as well as other persons responsible for implementing the procedures to which the documentation pertains.

HIPAA Security Plan Amendment

Plan Sponsor agrees that if it creates, receives, maintains, or transmits any electronic PHI (other than enrollment/disenrollment information and Summary Health Information, which are not subject to these restrictions) on behalf of the covered entity, it will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information, and it will ensure that any agents (including subcontractors) to whom it provides such electronic PHI agrees to implement reasonable and appropriate security measures to protect the information. Plan Sponsor will report to the Plan any security incident of which it becomes aware.

The Plan Sponsor will ensure that adequate separation between the Plan Sponsor and the Plan are supported by reasonable and appropriate security measures to the extent that the designees have access to electronic PHI.