

No: 209.1, 314.2, 414.2, 514.2

SECTION: PUPILS,
ADMINISTRATIVE,
PROFESSIONAL,
CLASSIFIED
EMPLOYEES

TITLE: HIPAA PRIVACY RULE

ADOPTED: December 1, 2003

REVISED:

PENN MANOR SCHOOL DISTRICT

209.1 HIPAA POLICY

I. Policy Statement

It shall be the policy of the Penn Manor School District to capture, share, secure, and maintain protected health information as defined from time to time by the HIPAA Privacy Rule in all mediums through appropriate information management policies and actions that meet applicable Federal, State, regulatory, or contractual requirements. Words and phrases defined in the Privacy Rule are used in this Policy with the same meanings as in the Privacy Rule.

II. Policy Purpose

The purpose of this Policy is to identify and disseminate the School District framework and principles for information management that guide our institutional actions and operations in protecting, generating, and sharing individually identifiable health information maintained by the School District for its students, employees, and other constituents.

III. Definition: Individually Identifiable Health Information

Any information, including demographic and/or scheduling information collected about an individual, that –

- a. Is created or received by a health care provider, health plan, employer, or any health care clearinghouse or any employee of the above; and
- b. Relates to the past, present or future physical and/or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

HIPAA PRIVACY RULE

- (i) Identifies the individual; or
- (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

All of the following are considered by the School District to fall into this category:

- Individual information collected by the School District nursing staff, athletic staff, support services, health plan, or other health care related services for which health information about individuals is collected (e.g., transferred medical records, correspondence, telephone calls, e-mail, etc.); or
- Patient information generated by any outside provider or contracted health plan or health care clearing house for the benefit of or dealing with a student, employee, or other individual as part of any program maintained or sponsored by the School District; or
- Information entrusted by the individual to a teacher, employee, vendor, volunteer, student, or other affiliate of the School District; or
- Any knowledge a teacher, staff member, employee, coach, vendor, volunteer, or other affiliate of the School District gains in the course of fulfillment of his or her appointed role in the School District regarding the individual; or
- Research information collected, generated, maintained, or disseminated by the School District that identifies individuals, or when combined with other data can reasonably lead to the identification of individuals.

A. General Standards

1. In order to protect the individually identifiable health information entrusted to the School District, no “protected health information” shall be disclosed by the School District except as permitted or required by Section 164.502(a) and (b) of the Privacy Rule.
2. All School District individually identifiable health information in any medium shall be maintained within the department constituting the health care component, or in a central depository for the School District under the control of the Privacy Officer.
3. All persons with access to School District individually identifiable health information may only have such access on a need to know basis and must be approved as an “authorized data user” prior to access thereto by the appropriate departmental head or by the Privacy

HIPAA PRIVACY RULE

Officer. Each separate health care component of the School District shall designate authorized data users for such component.

4. It is the responsibility of every authorized data user to maintain confidentiality of School District individually identifiable health information even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.
5. Each staff member, teacher, employee, trainee, student, vendor, volunteer, contractor, or other affiliate of the School District with access to School District individually identifiable health information is subject to and has the responsibilities outlined in this Policy.
6. Individually identifiable health information is the property of the individual to whom the information pertains and the School District is the steward of that information and the owner of the storage medium.
7. The department head, director, or manager (“Department Head”) of each health care component/department of the School District which constitutes the covered entity for purposes of School District compliance with the Privacy Rule shall be the data manager for that health care component. If no such position exists or if it is not clear where such responsibility lies, the Privacy Officer will identify a data manager for each health care component of the School District.

B. Personnel Designations

1. The Privacy Officer is responsible for the implementation of this Policy; the development from time to time of any appropriate amendments or additions to the Policy and its procedures; cataloging School District individually identifiable health information; receiving complaints; assisting the School District Community on the interpretation of this Policy; preparing and providing information regarding the School District Notice of Privacy Practices; monitoring and tracking violations and appeals; identifying areas of risk with the Information Security Committee; defining with the Information Security Committee security controls; training and education; and supervising maintenance of records of authorized data users with the Department Heads. The Privacy Officer shall have any additional duties set forth in the job description for Privacy Officer.
2. The Security Officer shall have the duties set forth in the Job Description – Information Security Officer.

HIPAA PRIVACY RULE

C. Complaints: Correction of Data

1. The Privacy Officer is responsible for all complaints. Individuals have the right to correct inaccurate individually identifiable health information. The appropriate process of validating and processing such corrections is initially determined individually by the Department Head of each covered health care function and is approved by the Privacy Officer.
2. Each Department Head is responsible for ensuring that validated correction requests relevant to School District individually identifiable health information under his/her control are implemented, subject to the general supervision and authority of the Privacy Officer.
3. To the extent that an audit trail shows access to an individual's individually identifiable health information, it shall be made accessible to that individual at the individual's request in the event that questions arise about improper access to his or her records.
4. The Privacy Officer shall document all complaints received and their disposition.

D. Safeguards and Security

1. The School District, through a committee ("Information Security Committee") chaired and convened by the Privacy Officer and composed of the Department Head of each health care component or other data manager designated by the Privacy Officer, shall create, administer and oversee policies to ensure the prevention, detection, containment, and correction of breaches of security, integrity, and confidentiality.
2. The security management process shall be the responsibility of the Department Head of each health care component under the general supervisory responsibility of the Privacy Officer, according to the guidelines set by the Information Security Committee, and must include, at a minimum, the implementation of:
 - a) Risk analysis, based on information asset contents and user population, to determine the likely occurrence and severity of loss of potential incidents.
 - b) Risk management including formal, documented procedures for monitoring, detection, auditing, reporting, and responding to breaches of security, integrity, and confidentiality.
 - c) A disciplinary process including procedures for the potential

HIPAA PRIVACY RULE

discipline, up to and including dismissal, for misuse, misappropriation of data, or acts of omission or commission which result in breaches of security, integrity, or confidentiality.

3. The prevention of access to School District protected health information by unauthorized or untrained personnel shall be addressed by personnel security policies, including provisions that:
 - a) Ensure that all personnel with access or potential access to School District protected health information are specifically authorized for that access, are trained in relevant School District confidentiality policies, and have attested knowledge of and compliance with those policies.
 - b) Ensure that operating and maintenance personnel are given the access necessary for them to perform their system maintenance responsibilities without compromising individually identifiable health information.
 - c) Ensure that personnel performing maintenance activities related to School District protected health information are supervised by authorized, knowledgeable persons.
 - d) Require maintenance of records of those granted physical access to School District protected health information.
 - e) Employ personnel security policy/procedures.
 - f) Ensure that system users, including technical maintenance personnel, are trained in system security.

4. The security management process shall be the responsibility of the Department Head of each health care component, according to the guidelines set by the Information Security Committee, and must include, at a minimum, formal, documented policies and procedures to limit physical access while ensuring that properly authorized access is allowed, including contingency planning for how security is to be maintained in the event of an emergency. These controls shall include, but not be limited to:
 - a) Applications and data criticality analysis.
 - b) A data backup plan.
 - c) Disaster recovery.
 - d) Emergency mode operation.
 - e) Equipment control (into and out of site) including workstation and laptop computers.
 - f) Procedures for verifying access authorizations prior to physical access.
 - g) Maintenance records.
 - h) Need-to-know procedures for personnel access.
 - i) Testing and revision.

HIPAA PRIVACY RULE

5. Certain individually identifiable health information, such as information regarding HIV, substance abuse, sexual abuse, mental health, and psychotherapy notes, are subject to additional specific legal restrictions. Disclosure to anyone other than the individual in question of such information shall only be made as permitted by this Policy and appropriate law.
6. The Privacy Officer shall evaluate and certify that appropriate security systems and measures have been implemented for each health care component.

E. Training

1. All applicable employees in each health care component of the School District shall receive education and training on the expectations, knowledge, and skills related to information security and the requirements of this Policy and the Privacy Rule prior to the compliance date of the Privacy Rule and upon any change in this Policy or the Privacy Rule, and in addition, as to new employees prior to being given access to School District protected health information. Department Heads of health care components of the School District shall verify and document the training and that employees under their supervision have received required education and training and attested to this Policy, and that they have attested to this Policy on an annual basis.
2. The employees of each covered function whose functions are affected by a material change to this Policy or by law shall receive training with respect to the Policy within a reasonable time after its implementation.

F. Sanctions and Mitigation

1. Should evidence of data access or disclosure of protected health information outside that granted and permitted under this Policy be discovered, it may result in disciplinary action, up to and including termination of employment.
2. Failure to follow the requirements of this Policy are subject to appropriate disciplinary action up to and including termination of employment.
3. All sanctions will be documented in accordance with School District employee policy.

HIPAA PRIVACY RULE

4. Each health care component of the School District shall mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of protected health information in violation of this Policy.

G. Notice of Privacy Practices

1. The School District's Notice of Privacy Practices is part of the Manual and is incorporated into this Policy.
2. The Privacy Officer is responsible for maintenance of the Notice of Privacy Practices.
3. The Notice of Privacy Practices shall be distributed to all students and employees of the School District on or before April 14, 2004, to each new student or employee upon enrollment or employment, and to others and otherwise to students and employees as and when required by law.