Policy

PROTECTED HEALTH INFORMATION

The District will, to the extent required by law, protect PHI (Protected Health Information) it receives about employees or other staff in a confidential manner as described in the Notice of Privacy Practices. Generally, only those with the need to know such information will have access to it, and even then, they will only have access to PHI to the Minimum Necessary for the legitimate use of the information. The District will comply with such other policies as it shall maintain from time to time with respect to the maintenance of such records. In response to the HIPAA Privacy Regulations, the District has adopted this policy which will apply to:

Hortonville Area School District Flexible Benefit Plan
Hortonville Area School Health Plan
Hortonville Area School District Dental Plan

These Plans are referred to collectively in this Policy as the "Health Plan". This policy will also apply to the District's employees, agents and service providers, to the extent required under applicable HIPAA Privacy Regulations. In addition, student education records as described in the Family Educational Rights and Privacy Act (FERPA) shall not be subject to the Policy.

Hortonville Area School District (the "District") recognizes that its Health Plan will be "Covered Entities" within the meaning of the privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (the HIPAA Privacy Regulations").

Implementation:

Privacy Officer
The Privacy Officer shall be the District Administrator.

Individual Health Plan participants and other interested parties are directed to contact the HIPAA Privacy Officer to: (1) file any internal or external complaint about HIPAA privacy related issues; (2) file a request for access or amendment to PHI; (3) inquire about any denial of access to PHI; or (4) make inquiry about any other matter regarding the District's policies and procedures related to the HIPAA Privacy Regulations.

General Policies Concerning Protected Health Information (PHI)

1. In accordance with the HIPAA privacy regulations, employment records will not be considered to be PHI, subject to HIPAA requirements unless specifically required by law. By way of example, the following employment records are not subject to the HIPAA Privacy Regulations: information obtained to determine an individual's suitability to perform his/her job duties (such as physical examination reports); drug and alcohol tests obtained in the course of employment, doctor's excuses provided in accordance with the District's attendance policy, work-related injury and occupational exposures reports and medical and laboratory reports related to such injuries or exposures, to determine worker's compensation coverage.

2. The District will provide each Hortonville Area School District Flexible Benefit Plan participant with a Notice of Privacy Practices. A notice of privacy practices related to the Hortonville Area School District Health Plan and Dental Plan will be provided by the insurer of such plans. The District will maintain a record to document its distribution of the Notice of Privacy Practices, but need not forward that document via certified or registered mail or obtain any signed acknowledgment of receipt from individual recipients.

3. Any individual employee who has a question about how his/her medical information is used and disclosed should contact the HIPAA Privacy Officer.

Access to PHI

Under the HIPAA Privacy Regulations, individuals have the right to access and to request amendment or restriction on the use of their own PHI. To ensure that the District only releases the PHI that is covered under the HIPAA Privacy Regulations, this Policy outlines procedures that interested individuals must follow to access, amend and restrict the use of their own PHI.

Participant/Beneficiary Access

1. An individual may request the individual's PHI.
2. Upon receipt of a completed request to inspect health information, the HIPAA Privacy Officer must verify the individual's identity (the use of driver's license, social security card or other formal identification is acceptable for this identification). If the request is received from a personnel representative, the representative's identity and authority to act on behalf of the individual should be verified. The HIPAA Privacy Officer should attach a note describing the documentation to the file copy of the request to inspect health information.
3. The Privacy Officer will act upon a verified request to inspect health information within thirty (30) days, preferably sooner. If the Privacy Officer cannot respond within thirty (30) days, the HIPAA Privacy Officer will provide a notice to the requestor within that thirty (30) day period explaining why the HIPAA Privacy Officer could not respond at that time and advising the individual that the HIPAA Privacy Officer will need an additional thirty (30) days to respond to the request.
4. The HIPAA Privacy Officer may deny an interested party access to PHI for any legally permissible reason, including, but not limited to the following:
    a. The information that the individual requested was compiled in reasonable anticipation of or for use in a civil, criminal or investigative administrative proceeding involving that individual;
    b. The information in the request was obtained from someone other than a health care provider and under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
    c. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the other person;

d. The protected health information makes reference to another person (other than a health care provider) and a licensed health care professional has determined in the exercise of professional judgment that the access requested is reasonably likely to cause substantial harm to that person;

e. The request for access has been made by a requester as a personal representative of the individual about whom the requestor is requesting the information and a licensed health care professional has determined under the exercise of professional judgment, that access by the individual is reasonably likely to cause harm to the other person.

5. If the HIPAA Privacy Officer denies a request to inspect health information, the Privacy Officer will provide the requesting party with a written notice stating the specific reason(s) for the denial. If an individual is denied access to PHI for any of the last three reasons listed above, then the individual may request a review of that denial by sending a written appeal request to the Privacy Officer. The District will designate a licensed health care professional who was not directly involved in the denial, to review the decision to deny patient access.
6. Access to actual files or computers that contain PHI should not be permitted. Rather, copies of such records should be provided to the individual requestor to view in a confidential area under the direct supervision of the HIPAA Privacy Officer. *Under no circumstances, should original PHI documents leave the District's premises.*

Request to Amend PHI

1. An interested party may request to modify his or her PHI records.
2. The Privacy Officer must act upon a request to correct or amend a record within sixty (60) days of receipt of such request. If the HIPAA Privacy Officer is unable to act upon the request within sixty (60) days, then it must provide the requestor with a statement of the reasons for the delay and provide the individual with a new response deadline (which cannot exceed an additional thirty (30) days).
3. The HIPAA Privacy Officer may deny a request to amend PHI for any legally permissible reason, including, but not limited to the following: (a) if any Health Plan did not create the PHI at issue; or (b) if the information is accurate.
4. If the Privacy Officer grants the request for amendment, the requestor should be provided a letter indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.
5. The individual requestor may be required to sign an authorization form in order for the District to notify affected parties that amendments have been made.
6. If the HIPAA Privacy Officer denies a request to amend a PHI record, the HIPAA Privacy Officer must provide the requestor with a written denial which must be written in plain language and state the reason for the denial; the individual's right to submit a statement disagreeing with the denial and how the individual may file such a statement; a statement that, if the individual does not submit a statement of disagreement, the individual may request that the Covered Entity provide the request for amendment and the denial with any future disclosure of PHI; and a description of how the individual may file a complaint with the Covered Entity, including the name and telephone number of an appropriate contact person or to the Secretary of Health and Human Services.

7. If an individual submits a "statement of disagreement," the HIPAA Privacy Officer may prepare a written rebuttal statement to the requestor's statement of disagreement. This statement of disagreement will be appended to the PHI and the summary of disagreement will be appended along with the rebuttal statement of the HIPAA Privacy Officer.
8. If the District receives a notice from another covered entity, that that entity has amended its own PHI in relation to a particular individual, then the District must amend its own PHI that may be affected by such amendments.

Requests for Restriction

1. An interested individual may request restrictions on the use or disclosure of his/her individual PHI.
2. The District is not required to agree to any request for restriction.
3. If the District agrees to a restriction, it may not use or disclose PHI in violation of the agreed upon restriction unless the individual who requested that restriction is in need of emergency service and the restricted PHI is needed to provide such emergency services.

Accounting of Disclosures of PHI

An interested individual may request an accounting of all accountable disclosures of his/her individual PHI made during the six years prior to the date of the request by providing the HIPAA Privacy Officer with a request for accounting of disclosures of PHI. However, no such accounting of disclosures will be made for any disclosures made: (1) to carry out treatment, payment or healthcare operations; (2) to individuals about their own PHI; or (3) pursuant to authorization.

The District will record any accountable disclosures. This includes information regarding: (1) the date of the disclosure(s); (2) the name(s) of the entity(ies) or the person(s) who receive the PHI and, if known, the address(es) of such entity or person; (3) a brief description of the PHI disclosed; and (4) a brief statement of the purpose of the disclosure.

Verbal Security

1. When transmitting PHI verbally, all employees of the District should do so in a secure or screened area (such as an empty conference room or closed office).
2. The District's staff members should be instructed and advised to not disclose or discuss PHI in any open area (e.g., hallway, break room, waiting room, etc.).
3. The District's staff members should only discuss PHI with those individuals who are involved in the Health Plan administration regardless of their physical location.
4. The District's staff members should be advised to be sensitive to the level of their voice and to the fact that others may be in a position to overhear some or all of their conversation.

Physical Security

1. PHI reports and records should be stored in safe and secure areas.
2. To the extent practical, all PHI records and reports will be placed in a locked file, out of common view. Individuals with a need to have access to that information for the completion of their job duties will have access, following a determination of such access. The HIPAA Privacy Officer will make a final determination as to which employees require access to that information.

3. Transfer of PHI records and data will be secured in a sealed envelope or box with explicit instructions regarding the appropriate individuals who may have access to that information.
4. PHI records, including all notes, remittance advices, charge slips or claims forms or enrollment material must not be left out in the open and should be stored in secure files or boxes that are secure and in an area where access is limited to those who need access to that information for the completion of their job duties.
5. Individual employees will be advised that they should not leave any records or reports that include PHI unattended at any location (e.g., on their desk, on a conference room table, or any other location).

Electronic PHI

Information that is stored electronically should be stored and maintained in a secure environment, in compliance with the District's other policies regarding the use of computers and other electronic devices.

Privacy Training

To ensure that the District's workforce, including (as required) all employees, volunteers, trainees, temporary employees, etc., (collectively, "staff") who have access to PHI understand the District's concern for the respect of employees' privacy. The District will provide those individuals with training regarding its privacy policies and procedures.

Enforcement

The HIPAA Privacy Officer is responsible for enforcing this Policy. All staff members are responsible for adhering to this Policy. Individuals who violate this Policy will be subject to the appropriate and applicable disciplinary process, up to and including termination of employment.

Definitions

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 involving the transmission of information between two entities.

Minimum Necessary

When using or disclosing PHI or when requesting PHI from another Covered Entity, the District must limit PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure or request. Minimum Necessary does not apply in the following circumstances:

a. Disclosures by a health care provider for treatment (students and trainees are included as health care providers for this purpose);
b. Uses and disclosures based upon a valid authorization to use and disclose PHI;
c. Disclosures made to the Secretary of Health and Human Services;
d. Uses and disclosures required by law; and
e. Uses and disclosures required by other sections of the HIPAA Privacy Regulations.

PHI

PHI is defined under the HIPAA Privacy Regulations, and generally includes all "individually

identifiable health information" that is transmitted or maintained in any form or medium by a Covered Entity. This can include oral discussions, paper documents and computerized information. "Individually identifiable health information" is defined as health information that is:

a. Created or received by a health care provider, health plan, life insurer, school, university, public health authority, employer or health care clearinghouse;
b. 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 the past, present or future payment for the provision of health care to an individual; and
c. Identifies the individual or creates a reasonable basis to believe it would identify the individual.

Associated Information: 45 Code of Federal Regulations Parts 160 and 164