HIPAA

Note:

(1) Any school district offering a group "health care plan" for its employees is affected by HIPAA. School districts offering health plans that are self-insured will be entirely responsible for compliance with HIPAA, despite a third party administrator managing the plan. School districts may also be subject to HIPAA as a "health care provider" by either having a school-based health center or a school nurse. School-based health centers staffed and serviced by a hospital or local health department are responsible for complying with HIPAA if there is a sharing of records containing health information. For those districts providing the services of a school nurse, HIPAA regulations issued in 2000 commented that an "educational institution that employs a school nurse is subject to [the] regulations as a health care provider if the school nurse or the school engaged in a HIPAA transaction." This transaction occurs when a school nurse submits a claim electronically.

(2) Any personally identifiable health information contained in an "education record" under FERPA is subject to FERPA, not HIPAA.

Background

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The District's group health plan is a Covered Entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, the Standards for the Privacy of Individually Identifiable Information. In order to comply with HIPAA and its related regulations, the District has implemented the following HIPAA Privacy Policy:

The HIPAA Privacy Rule

HIPAA required the federal government to adopt national standards for ***electronic health care transactions***. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information and determined there was a need for national privacy standards. As a result HIPAA included provisions which mandated the adoption of federal privacy standards for individually identifiable health information.

The standards found in the Privacy Rule are designed to protect and guard against the misuse of individually identifiable health information, with particular concern regarding employers using an employee's (or dependent's) health information from the group health plan to make adverse employment-related decisions. The Privacy Rule states that verbal, written, or electronic information that can be used to connect a person's name or identity with medical, treatment, or health history information is Protected Health Information (PHI) under the HIPAA Privacy Rule.

Under the HIPAA Privacy Rule:

1. Individuals have a right to access and copy their health record to the extent allowed by HIPAA.

2. Individuals have the right to request an amendment to their health record. The plan may deny an individual's request under certain circumstances specified in the HIPAA Privacy Rule.

3. Individuals have the right to an accounting of disclosures of their health record for reasons other than treatment, payment, or healthcare operations.

4. PHI, including health, medical, and claims records, can be used and disclosed without authorization for specific, limited purposes (treatment, payment, or operations of the group health plan). A valid authorization from the individual must be provided for use or disclosure for other than those purposes.

5. Safeguards are required to protect the privacy of health information.

6. Covered entities are required to issue a notice of privacy practices to their enrollees.

7. Violators are held accountable with civil and criminal penalties for improper use or disclosure of PHI.

Compliance

The Superintendent has been designated Privacy Officer. The Privacy Officer will oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to the District's policies and procedures covering the privacy of and access to patient health information in compliance with HIPAA, other applicable federal and state laws, and the District's privacy practices.

As required for a Covered Entity under HIPAA, the plan has developed these internal privacy policies and procedures to assure that PHI is protected and that access to and use and disclosure of PHI are restricted in a manner consistent with HIPAA's privacy protections. The policies and procedures recognize routine and recurring disclosures for treatment, payment, and healthcare operations and include physical, electronic, and procedural safeguards to protect PHI. The procedures include safeguards for sending PHI via mail or fax, receiving PHI for plan purposes, and workstation safeguards and procedures for securing and retaining PHI received by the plan. Plan participants are entitled to receive a copy of the plan's policies and procedures upon request.

Designating a limited number of privacy contacts allows the District to control who is receiving PHI from the contract claims payor for plan operations purposes. The contract claims payor will provide only the minimum PHI necessary for the stated purpose and, as required under the Privacy Rule, will provide PHI only to individuals with a legitimate need to know for plan operations purposes.

The District has distributed a notice of privacy practices to plan participants. The notice informs plan participants of their rights and the District's privacy practices related to the use and disclosure of PHI. A copy of this notice may be obtained by contacting the Privacy Officer.

The District has reviewed how PHI is used and disclosed by the plan and has limited disclosure of that information to employees who have a legitimate need to know or possess the PHI for healthcare operations and functions. The District will make reasonable efforts to use de-identified information whenever possible in the operations of the plan and will only use the minimum PHI necessary for the stated purpose.

Some of the District's employees need access to PHI in order to properly perform the functions of their jobs. The District has identified these employees and has given them training in the important aspects of the HIPAA Privacy Rule, the privacy policy, and procedures. New employees who will have access to PHI will receive training on the HIPAA Privacy Rule and related policies and procedures as soon as reasonably possible after they are employed. Employees who improperly use or disclose PHI or misuse their access to that information may be subject to discipline, as deemed appropriate.

In the event the group health plan must disclose PHI in the course of performing necessary plan operations functions or as required by law or a governmental agency, the District has developed a system to record those disclosures and requests for disclosures. An individual may request a list of disclosures of his or her PHI made by the plan for other than treatment or claims payment purposes. All requests for an accounting of PHI disclosures must be made in writing, and the plan may impose fees for the cost of production of this information. Requests will be responded to within sixty (60) days. If the plan is not able to provide the requested information within sixty (60) days, a written notice of delay will be sent to the requesting individual, with the reasons for the delay and an estimated time for response.

In order to comply with the new privacy regulations, the plan has implemented compliant communication procedures. Except for its use in legitimate healthcare operations, written permission will be required in order for the District to disclose PHI to or discuss it with a third party.

The HIPAA Privacy Rule prohibits the District from disclosing medical information without the patient's written permission other than for treatment, payment, or healthcare operations purposes. An authorization signed by the patient and designating specified individuals to whom the District may disclose specified medical information must be on file, before the plan can discuss a patient's medical information with a third party (such as a spouse, parent, group health plan representative, or other individual).

The District has taken the following steps to ensure PHI is safeguarded:

- The District has implemented policies and procedures to designate who has and who does not have authorized access to PHI.

- Documents containing PHI are kept in a restricted/locked area.

- Computer files with PHI are password protected and have firewalls making unauthorized access difficult.

- Copies of PHI will be destroyed when information is no longer needed, unless it is required by law to be retained for a specified period of time.

- The District will act promptly to take reasonable measures to mitigate any harmful effects known to the group health plan, due to a use or disclosure of PHI in violation of the plan's policies, procedures, or requirements of the HIPAA Privacy Rule.
- The District will appropriately discipline employees who violate the District's group health plan's policies, procedures, or the HIPAA Privacy Rule, up to and including termination of employment if warranted by the circumstances.

The District has received signed assurances from the plan's business associates that they understand the HIPAA Privacy Rule, applicable regulations, and the Privacy Policy and will safeguard PHI just as the plan would.

The contract claims payor and certain other entities outside the group health plan require access on occasion to PHI, if they are business associates of the group health plan and in that role need to use, exchange, or disclose PHI from the group health plan. The plan requires these entities to sign an agreement stating they understand HIPAA's privacy requirements and will abide by those rules just as the group health plan does, to protect the PHI to which they have access. For example, the plan engages a certified public accountant to audit the plan annually and to make sure payments are made in compliance with the Plan Document. In order for the CPA to complete an audit, the auditor reviews a sample of the claims for accuracy.

The District will ensure health information will not be used in making employment and compensation decisions. The HIPAA Privacy Rule and other applicable laws expressly prohibit an employer from making adverse employment decisions (demotions, terminations, etc.) based on health information received from the group health plan. To the extent possible, the District has separated the plan operations functions from the employment functions and has safeguards in place to prevent PHI from the plan from going to or being used by an employee's supervisor, manager, or superior to make employment-related decisions.

Complaints

If an employee believes their privacy rights have been violated, they may file a written complaint with the Privacy Officer. No retaliation will occur against the employee for filing a complaint. The contact information for the Privacy Officer is:

Tom Stack, Superintendent
Bigfork School District #38
PO Box 188
Bigfork, MT 59911

Legal Reference: 45 C.F.R. Parts 160, 162, 164

Policy History:
First reading on: 12/8/21
Second reading/Adopted on: 1/12/22