Pinellas County Schools

HIPAA Frequently Asked Questions

What is Protected Health Information?

Protected Health Information or PHI is medical records or other health information that identifies (or reasonably could be used to identify) an individual, and relates to a past, present or future physical or mental health condition of the individual, or the payment of health care for that individual. This "individually identifiable health information" can be in any form (i.e., electronic, written or oral) and is created or received by a HIPAA covered entity (i.e., a health plan, health care provider, or health information clearinghouse) or by an employer.

What is meant by individually identifiable information?

Individually identifiable information includes data about a person that could be used to identify that person. Typical "identifiers" may include:

- Patient name
- Medical records number
- Health plan beneficiary numbers
- Address, zip code
- Phone number, email address, fax number, Internet Protocol address
- License numbers
- Full face photographic images
- Social Security number

Is Protected Health Information usually a written document?

No, Protected Health Information can be any form – written on paper, displayed or stored in a computer, or spoken in conversation.

What is the difference between a Covered Entity and Business Associate?

Covered Entities are organizations that are required by HIPAA's Privacy Rule to protect the confidentiality of PHI and ensure individuals' rights regarding their PHI are respected. These include health care providers, health care plans and health care clearinghouses.

Business Associates are the external vendors or professionals that perform duties on behalf of covered entities. For example, a third party administrator (TPA) hired by an employer in its role as health plan sponsor to perform claims payment duties for a self-funded health plan would be a Business Associate.

NOTE: Pinellas County Schools is neither a Covered Entity nor a Business Associate.

Are employers considered Covered Entities?

No. However, a few employers may be Covered Entities under certain, limited circumstances (e.g., employer that operates an on-site health clinic).

How does the law define group health plans?

The HIPAA Privacy Rule defines a health plan as a group health plan, whether insured or self-funded, that has 50 or more participants or is administered by a third party. This would include medical, dental and vision plans; HMOs, PPOs, insurers and health care flexible spending accounts. Disability, workers' compensation and life insurance plans are *not* health plans subject to HIPAA's Privacy Rule.

What are an employer's obligations under the HIPAA Privacy Rule?

Although not directly subject to the Privacy Rule as Covered Entities, employers need to assess the effect of HIPAA on their health plan(s) and their human resource operations. This affects several areas, including:

1. Ensuring that all the sponsor's health plans are HIPAA-compliant, including obtaining assurances from Business Associates that they will comply with the Privacy Rule by the compliance date, April 14, 2003 [e.g., need to make sure Business Associate Agreements, where necessary, are in place.]
2. Reviewing the collection, storage and use of PHI within day-to-day operations to ensure compliance with the Privacy Rule and protect the rights of employees under HIPAA.

What specifically must employers do to comply?

To comply with the HIPAA Privacy rule, employers who are health plan sponsors must:

- Have their insurance carriers provide a notice to employees and participants in their covered health plans that describes the health plan's privacy policies and procedures; individual's health information privacy rights under HIPAA and how PHI may be used or disclosed by the employer's health plan(s)
- Develop and implement privacy policies and procedures to safeguard PHI
- Designate a Privacy Officer and/or Associate Privacy Officers
- Amend plan documents for the Privacy Rule
- Train employees on the plan sponsor's privacy policies and procedures
- Ensure that plans are HIPAA-compliant and sign Business Associate Agreements, where necessary, with their health plan vendors by April 14, 2003
- Review the collection, storage and use of PHI within day-to-day operations
- Establish appropriate safeguards to protect the privacy of PHI.

Are employment records subject to the privacy standards?

Generally, no. Employment records, including medical information that an employer needs to carry out its obligations under FMLA, ADA and similar laws, as well as records related to occupational injury, disability eligibility, sick leave requests, drug screening results and fitness-for-duty tests, are not considered PHI subject to the Privacy Rule.

What information needs to be included in the HIPAA Privacy Notice?

Group health plans must provide participants with a statement of the:

- Intended use or disclosures of PHI
- Individual's right to request restrictions on the plan's use or disclosure of PHI
- Duty of the Covered Entity to comply with the privacy standards and its own privacy practices
- Individual's right to file a complaint if privacy violations are suspected
- Name, title and phone number of the contact person for receiving complaints.

Who must issue the HIPAA Privacy Notice?

Self-funded health plans must issue their own Privacy Notices. However, the Privacy Rule allows these plans to contract this function out to a "Business Associate." For fully insured plans, the obligation to issue the notice rests with the insurer. As plan sponsor, the employer should check with its insurers (or TPA in the case of self-funded plans) to ensure the notice requirement is fulfilled in the designated timeframe.

When must it be provided?

The Health Privacy Notice must be provided to all plan members whose PHI will be used or disclosed by the plan no later than April 14, 2003 (small health plans, those with annual receipts of $5 million or less, have until April 14, 2004 to comply). Also, notices must be given to new health plan participants at enrollment time and to all enrollees within 60 days after the notice is materially changed. Thereafter, plans must advise that the notice is available at least once every three years.

When is individual authorization required for disclosure of health information?

Covered Entities must obtain an individual's authorization to use or disclose that person's protected health information for non-routine purposes, such as for employment decisions and eligibility or enrollment determinations, or other non-health purposes. Individual authorization is *not* required for routine use or disclosure. This allows health plans, health care clearinghouses and health care providers to use and disclose health information for routine health care treatment, payment or health plan operations without first obtaining a patient's authorization.

Under HIPAA, an authorization is an individual's permission for a Covered Entity (e.g., health plan) to use PHI for specified purposes, other than for payment, treatment or operations, or to disclose PHI to a third party.

What are examples of permissible PHI disclosures?

HIPAA permits health plans to use or disclose PHI without an individual's authorization for the following purposes:

- Disclosure of PHI for health care treatment, plan payment (claims or premium payments), or health plan operations (TPO)

- Disclosure of PHI to Business Associates provided the Business Associate has agreed to safeguard the information
- Disclosure of de-identified Summary Health Information to the plan sponsor for the purpose of obtaining a premium bid or amending or terminating a health plan
- Disclosure of de-identified health information to a plan sponsor
- Disclosure of PHI to plan sponsors if the sponsor has amended the health plan document to restrict its use in a manner consistent with the HIPAA rules.

Note that under HIPAA, whether or not an individual's authorization is required in a particular circumstance to use or disclose PHI, only the "minimum necessary" amount of information to accomplish the intended purpose can be disclosed.

What are some examples of TPO?

A health plan can disclose PHI without authorization for treatment, payment or health care operations (TPO). This includes quality assessment, case management, claims adjudication, utilization review, audits, underwriting, premium rating, and other activities related to creation, renewal or replacement of health insurance (including stop-loss).

What is meant by "de-identified" information?

PHI is considered de-identified if all identifying information has been removed and there is no reasonable basis to believe that the information can be used to identify an individual. To de-identify information the following data would be removed:

- Name
- All geographic subdivisions smaller than a state (e.g., street address, city, zip code)
- All elements of dates (except year) related to an individual (e.g., birth date, admission date) and all elements of dates indicative of age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical records numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images, and
- Any other unique identifying number, characteristic or code.

What type of recordkeeping is required to comply with the HIPAA Privacy Rule?

Health plans must develop and implement a record retention system that provides for retention of copies of all notices, consents, authorizations, designations, policies and procedures. For example, the system must be able to accommodate individuals' right to receive an accounting of disclosures of their PHI (not made for TPO or requested by the individual him or herself). This right to an accounting applies to disclosures made during the prior six (6) years.

NOTE: Pinellas County Schools is not a health plan.

Describe the training required by HIPAA's Privacy Rule.

Anyone (e.g., plan sponsor employees) who may be exposed to or who will encounter PHI in the performance of their normal job functions must receive training that covers the health plan's privacy policies and procedures. This would typically include:

- Human resources and benefits administration staff
- Managers and supervisors
- IT staff
- Employee Benefits Privacy Officer and anyone who has been specifically authorized to use/disclose PHI.

What do I do if my state has privacy laws that differ from HIPAA's requirements?

HIPAA's Privacy Rule provides a federal floor of safeguards to protect the confidentiality of personal medical information. State laws that provide stronger privacy protection and do not conflict with HIPAA will apply over and above the new federal privacy standards.

What are the responsibilities of the Employee Benefits Privacy Officer?

The Employee Benefits Privacy Officer is responsible for overseeing the process for protecting the privacy and confidentiality of health information. These responsibilities include establishing the health plan's privacy policies and procedures, training affected staff in those policies and procedures, and collecting release/authorization forms to ensure HIPAA compliance. The Employee Benefits Privacy Officer is also the internal resource for questions concerning the Privacy Rule.

What is EDI?

Electronic data interchange (EDI) is the electronic transfer of health information, such as claims data, between service providers, such as between health care providers and claims processors. Originally scheduled to apply to large group health plans (those with annual receipts of more than $5 million) October 16, 2002, compliance with the EDI standards was delayed for one year provided the health plan submitted a model compliance form to HHS by October 15, 2002. Thus, for most plans, the EDI rules will go into effect on October 16, 2003 (this includes small health plans with annual receipts of $5 million or less).

The EDI rules will allow medical information to be transferred more quickly and cost effectively through the use of uniform transaction data formats and medical code sets on a national basis.

What types of data are covered by the EDI standards?

EDI standards cover the following electronically transmitted data between Covered Entities:

- Health care claims
- Claims status requests
- Health care payments
- Participant enrollment/disenrollment
- Health plan premium payments
- Participant eligibility
- Referral certification and authorization
- Coordination of benefits.

What happens if we don't comply?

Violating the HIPAA Privacy Rule can result in stiff penalties. Both civil and criminal penalties for noncompliance, enforced by the Department of Health and Human Services, may apply. These are as follows:

- Civil penalties – $100 fine per person, per violation, up to $25,000 per person/year
- Criminal penalties – Up to $250,000 fine and 10 years in