

HIPAA Privacy Rule

OVERVIEW

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 includes a federal regulation called the Privacy Rule, which was issued to protect the privacy of certain medical information that may identify an individual. Any medical information that may identify an individual is known as *protected health information* (PHI).

Other Products Of Interest

- [Paychex Direct Catalog](#)
- [Paychex PremierSM Human Resources](#)

The Privacy Rule governs the way *covered entities* may use and disclose PHI for administrative purposes. A covered entity subject to the Privacy Rule may not use or disclose PHI, except as authorized by the individual who is the subject of the PHI, or as permitted under the Privacy Rule. Most covered entities had to comply with the Privacy Rule by April 14, 2003; however, small group health plans had an extra year to comply. This brochure is intended to provide the reader with a basic understanding of the Privacy Rule. It is intended for informational purposes only and is not legal advice. Because of the complexity of the Privacy Rule, the reader should seek professional advice from an attorney before acting on any information contained in this publication.

REQUIREMENTS OF COVERED ENTITIES

The Privacy Rule requires every covered entity to comply with certain administrative and organizational requirements and safeguards. The requirements set forth below represent some, but not all, of the covered entity's obligations under the Privacy Rule:

Designated Privacy Official – Covered entities must designate one qualified individual to develop and implement its privacy policies and procedures, along with a designated contact person to provide individuals with information pertaining to the entity's privacy practices and to receive complaints. The contact person may be, but is not required to be, the same as the *privacy official*.

Privacy Awareness Training – All workforce members who are likely to have access to PHI must be trained on the company's privacy policies and procedures as necessary to be able to perform their functions within the entity. Workforce members include employees, volunteers, trainees, and any other individuals under the direct control of the entity. Training must be provided for new members within a reasonable time after joining the entity. Covered entities must also retrain any members affected by significant changes made to the entities' policies or procedures within a reasonable time after the change is made. Training efforts must be documented.

Security Standards and Safeguards – A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. The Privacy Rule details the security and administrative safeguards that must be implemented.

Complaint Procedures – Covered entities must establish procedures for individuals to file complaints pertaining to its privacy practices. Complaint procedures must be explained in the entity's *privacy practices notice*. Additionally, a record of complaints received and a brief explanation of all resolutions must be maintained.

Procedures for Violations – Covered entities must administer appropriate sanctions against workforce members who violate its privacy policies and procedures under the Privacy Rule. Disciplinary action taken will vary depending on factors such as the nature (i.e., accidental vs.

intentional disclosure) and severity of the violation, whether the violation indicated a pattern or practice of improper use or disclosure, etc. Sanctions may range from a warning to termination.

Duty to Mitigate – Covered entities must attempt to diminish (to the extent possible) any harmful effects caused by the inappropriate use or disclosure of PHI by its workforce or *business associates*.

No Retaliation – Covered entities are prohibited from intimidating, threatening, coercing, discriminating against, or taking any retaliatory action against any individual for exercising their rights under the Privacy Rule; testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the regulation; or opposing any act or practice that the person, in good faith, believes is in violation of the Privacy Rule.

Waiver of Rights – Covered entities cannot require individuals to waive any of their rights under the Privacy Rule as a condition of obtaining treatment, payment, enrollment in the plan, or benefits eligibility.

Written Policies and Procedures – Covered entities must establish and execute written privacy policies and procedures with respect to the Privacy Rule.

Documentation – Any documentation required under the Privacy Rule must be retained for at least six years from the date the documentation was created, or the date when it was last in effect, whichever is later. Additional information regarding the requirements of a covered entity can be found on the Department of Health and Human Services (HHS) Web site at www.hhs.gov/ocr/hipaa.

SELF-FUNDED PLAN REQUIREMENTS

There are specific privacy requirements for self funded and self-administered plans. The extent of the plan's HIPAA requirements will depend upon the amount of access the company has to the plan participants' PHI. Such requirements are covered in the regulations, and plan sponsors of self-funded and self-administered plans should work with their legal counsel to ensure compliance for their specific plan(s). Additional information is also available on the HHS Web site at www.hhs.gov/ocr/hipaa.

ENFORCEMENT AND PENALTIES

The Privacy Rule provides a process whereby an individual can file a complaint with the HHS. The Privacy Rule also describes the responsibilities of covered entities to provide information, and cooperate with any investigations and compliance reviews. HHS may impose civil monetary penalties against covered entities amounting to \$100 per incident for failure to comply with the Privacy Rule requirements. (Penalties may not exceed \$25,000 per calendar year for multiple violations of the same Privacy Rule regulation.) HHS may not impose a civil monetary penalty under certain circumstances, as long as the covered entity corrected the violation within 30 days of when it knew (or should have known) of the violation. Criminal penalties may be imposed on an individual who knowingly discloses or obtains *individually identifiable health information*. This penalty could result in a fine of \$50,000 and up to one year imprisonment. The penalty may be increased to \$100,000 and up to five years imprisonment if the violation involves false pretenses. If the violation involves the intent to sell, transfer, or use information for personal or commercial gain, or is malicious in intent, the penalty may be as high as \$250,000 and up to ten years imprisonment.

FREQUENTLY ASKED QUESTIONS

Q: What does it mean if my company is considered a business associate?

A: If it has been determined that a business associate relationship does exist, then a Business Associate Agreement is required. Under the contract, a covered entity is required to impose specified written safeguards on the PHI used or disclosed by its business associates.

Q: Are employers with fully insured health plans required to comply with these administrative requirements?

A: Employers who provide health insurance benefits through fully insured plans (and do not create, receive or maintain protected health information other than summary health information or information regarding enrollment) are not covered entities as defined by HIPAA. However, the employer, as the plan sponsor, may have certain compliance requirements depending on the information they receive from a covered entity.

Q: Where can I obtain more detailed information regarding the HIPAA Privacy Rule?

A: The Department of Health and Human Services has information on their Web site regarding the Privacy Rule. It includes a HIPAA fact sheet, questions and answers, and access to the regulations contained in the Privacy Rule. The Web address is www.hhs.gov/ocr/hipaa. You may also call them toll free at (866) 627-7748.

PAYCHEX PRODUCTS AND THE PRIVACY REGULATION

Section 125 Plans

A section 125 plan is a fringe benefit plan. The fringe benefit plan itself is not bound by the HIPAA Privacy Rule. However, some of the underlying benefits offered by the plan (i.e., health insurance, health flexible spending account, etc.) are bound by the Privacy Rule. The employer, acting as a plan sponsor, may have a variety of compliance concerns, based on the structure of their benefit plans. For example, if the benefits offered under the plan are self-funded, the employer, as a plan sponsor, will have additional requirements regarding the use and disclosure of participants' PHI. If the employer outsources the administration or recordkeeping of these plans, they will need to ensure that their third party administrator, or any other outside vendor, is taking the necessary steps to comply with the regulations. This is typically accomplished via a Business Associate Agreement provided by the plan administrator or vendor. Paychex is considered a business associate of clients who utilize them for the recordkeeping of their health flexible spending account plan.

Employee Handbooks

While employers have certain obligations when complying with HIPAA, in general, individual employees do not. Accordingly, the Paychex database of handbook policies does not have a policy that addresses HIPAA as part of our standard database.

GLOSSARY

Business Associate – In general, a person or organization, other than a member of the covered entity's workforce, which performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of protected health information (PHI). Examples of these functions include claim processing, data analysis, utilization review, and billing. If the person's or organization's function does not involve the use or disclosure of PHI, or any incidental access to PHI, then they are not considered a business associate.

Covered Entity – A health plan, health care clearinghouse, or health care provider that electronically transmits certain health care information. An employer who is also an administrator or plan sponsor with access to protected health information is considered a covered entity.

De-identified Health Information – Health information classified as "de-identified" is stripped of all identifying data which would enable someone to identify the individual. There are two ways to de-identify information: 1) a qualified statistician makes a formal determination; or 2) certain identifiers of an individual are removed, as well as those of the individual's relatives, household members, and employers, in accordance with the Privacy Rule, so that the covered entity would have no actual knowledge that the remaining information could be used to identify the individual.

Health Care Clearing House – A covered entity that processes nonstandard information received from another party into standard information (or vice versa). Examples of health care clearing houses include billing services, repricing companies, and community health management information systems.

Health Care Provider – A covered entity that provides services and electronically transmits information in connection with certain transactions such as claims, benefit eligibility inquiries, or referral authorization requests. Providers of services include, but are not limited to, hospitals, physicians' offices, and any other person or organization that furnishes, bills, or is paid for health care.

Health Plan – A covered entity such as an individual or group health plan, that provides or pays the cost of medical care. Self-administered group health plans with less than 50 participants are not subject to the Privacy Rule.

Individually Identifiable Health Information – Any information that is created or received by a covered entity that relates to the following:

- The individual's past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past, present, or future payment for the provision of health care to the individual, and that identifies or creates a reasonable basis to believe that it can be used to identify the individual.

Individually identifiable health information includes many common identifiers including but not limited to:

- Name
- Address
- Photographs
- Social security number
- Email addresses
- Any individually identifying number, characteristic, or code

Privacy Official – A qualified individual designated by the covered entity to develop and implement its privacy policies and procedures.

Privacy Practices Notice – A statement or notice by a covered entity that explains the ways in which protected health information (PHI) is used and disclosed, as well as the individual's rights regarding their PHI. It must include the following:

- The covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice;
- The rights of the individuals, including the right to complain to the Department of Health and Human Services (HHS) and to the covered entity if they believe their privacy rights have been violated;
- Procedures for filing a complaint to the HHS if an individual feels their privacy has been violated; and
- A point of contact for further information and for making complaints to the covered entity.

Additional information regarding Privacy Practices Notice requirements can be found on the HHS Web site at www.hhs.gov/ocr/hipaa.

Protected Health Information (PHI) – Any individually identifiable health information that is transmitted or maintained by electronic media or in any other form or medium. Employment records held by a covered entity in its role as an employer are not considered PHI.