# Health Insurance Portability and Accountability Act Privacy Rule

Fact Sheet

## Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] enacted changes in the health insurance market and addressed the electronic transmission of health information and the protection of personal health information, among other things. HIPAA, and specifically the Privacy Rule, have had a significant impact on the public health community's access to health data and when and how such data is shared with and by public health agencies. (See ASTHO *Public Health Access to Student Health Data Issue Brief* for a detailed analysis of HIPAA.)

## What the Law Does

Title II of HIPAA contained a number of administrative simplification and privacy provisions that instructed the Secretary of Health and Human Services (HHS) to issue standards addressing, among other things, the electronic transmission of health information and the privacy of personally identifiable medical information.[2] HIPAA and the rules implementing it have been amended frequently since its original passage in 1996. In 2000, HHS promulgated *Standards for Privacy of Individually Identifiable Health Information* (known as the "Privacy Rule") and then issued modifications to the rule in 2002.[3] The HIPAA Privacy Rule creates a set of basic consumer protections and a series of regulatory permissions for uses and disclosures of protected health information.[4] This fact sheet focuses on the HIPAA privacy requirements currently enacted.

### *Liability and Enforcement*

The Privacy Rule does not authorize individuals to sue for violations; individuals must direct their complaints to HHS's Office for Civil Rights (OCR), which then investigates the complaint. In cases of noncompliance, the Secretary is directed to resolve the matter by informal means.[5] If the matter cannot be resolved informally, the Secretary may issue written findings of noncompliance that may be used as a basis for initiating a civil action or a criminal case.[5] Violators that knowingly and improperly disclose identifiable health information are subject to civil monetary and criminal penalties.[5]

## How the Law Works

The HIPAA Privacy Rule prohibits covered entities from disclosing protected health information to any third parties, unless the rule otherwise permits the disclosure.[4]

- ***Covered Entities***—The Privacy Rule applies to "covered entities," which are health plans, healthcare clearinghouses, and any healthcare provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.[5] A "business associate" is a person or organization who is not employed by the covered entity who performs certain activities for a covered entity that involve the use or disclosure of individually identifiable health information.[5] A "hybrid entity" is an entity that conducts both covered and noncovered activities under the Privacy Rule.[5] State and local health departments can be hybrid entities if they provide healthcare services to patients for which the agencies transmit health information electronically in addition to conducting their other public health functions.
- ***Protected Health Information***—The Privacy Rule applies to protected health information (PHI), which is individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media—electronic, paper, or oral.[3] PHI includes demographic data; common identifiers (e.g., name, address, birth date, Social Security Number); information relating to the individual's past, present, or future physical or mental health condition, healthcare provided to them, or payment for healthcare; and data that identifies the individual or that could be reasonably used to identify the individual.[5] Employment records maintained by a covered entity for its own employees and education records covered by the Family Educational Rights and Privacy Act (FERPA) are specifically excluded from the definition of PHI.[5] (See ASTHO *FERPA Fact Sheet*.) There are no restrictions on the use or disclosure of de-identified health information.[5]
- ***Disclosures***—A covered entity may not use or disclose PHI, except either as the Privacy Rule permits or requires, or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[5] Disclosure is required to be made to the individual/representative or to HHS as part of an enforcement action.[5] A covered entity is permitted, but not required, to use and disclose PHI, without an individual's authorization, for the following purposes or situations: (1) to the individual; (2) for treatment, payment, and healthcare activities like quality assessment or evaluations; (3) informal opportunities to agree or object such as providing information for hospital directories or notifications to family members; (4) disclosures incident to an otherwise permitted use and disclosure; (5) public interest and benefit activities; and

(6) the use or disclosure of limited data sets for the purposes of research, public health, or healthcare operations.[5] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.[5]

### *Disclosures for Public Interest and Benefit Activities*

The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization, for a dozen enumerated public purposes.[5] These disclosures are permitted, but not required, in recognition of the important uses made of health information beyond the realm of healthcare. Specific conditions or limitations apply to each public interest purpose. Several of these exceptions are described below:

- ***Public Health Activities***—Covered entities may disclose PHI to: (1) public health officials authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability; (2) public health or other government officials authorized to receive reports of child abuse and neglect; (3) entities subject to FDA regulation regarding FDA-regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (4) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (5) employers requesting information regarding their employees for work-related illness or injury or workplace-related medical surveillance because the information is needed to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state requirements.[5]
- ***Serious Threat to Health or Safety***—The Privacy Rule allows covered entities to disclose PHI that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).[5] Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or criminal.[5]
- ***Judicial and Administrative Proceedings***—The Privacy Rule permits covered entities to disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal.[5]

### *Waivers of HIPAA During Emergencies*

Federal law provides for the waiver or modification of certain HIPAA requirements during emergencies. Section 1135 of the Social Security Act (SSA) authorizes the HHS Secretary to temporarily modify or waive certain Medicare, Medicaid, State Children's Health Insurance (SCHIP), and HIPAA requirements.[15] SSA Section 1135 addresses, among other things, the waiver of sanctions arising from noncompliance with HIPAA privacy regulations relating to: (1) obtaining a patient's agreement to speak with family or friends or honoring a patient's request to opt out of the facility directory; (2) distributing a notice of privacy practices; or (3) the patient's right to request confidential communications. (See ASTHO Fact Sheet *Social Security Act §1135 Waivers*.)

**Practice Notes**

- Identify the student health data needed and if it involves PHI.
- Identify sources for the data, such as school health data not covered by FERPA and data from providers.
- Determine if the data is covered by HIPAA or other federal and state privacy laws.
- If HIPAA or other laws apply, determine if any exception applies.
- If not, identify and obtain required consents, or use limited data sets or de-identified data.

## How the Law Affects States

In general, any state laws or regulations that conflict with HIPAA and the Privacy Rule are preempted by the federal law, and the federal requirements control over the state requirements. The Privacy Rule contains exceptions that allow differing state requirements to control if the state law: (1) relates to privacy of individually identifiable health information and provides greater protections or rights than the Privacy Rule; (2) requires the reporting of disease, injury, child abuse, birth, or death, and for public health surveillance, investigation, or intervention; or (3) requires certain reporting by health plans, such as for management or financial audits or evaluations.[5] States can also request a determination that a conflicting state law will not be preempted by HIPAA if the state can demonstrate one of the conditions listed in the rule, including, but not limited to, that the conflicting provision serves a compelling public health, safety, or welfare interest, and, if the conflicting provision relates to a privacy right, that the intrusion into privacy is warranted given the public interest being served.[5]

---

*Sources:*

[1] Health Insurance Portability and Accountability Act (HIPAA) of 1996. (P.L.104-191).

[2] Chaikind H et al. Congressional Research Service. *The Health Insurance Portability and Accountability Act (HIPAA) of 1996: Overview and Guidance on Frequently Asked Questions* (RL31634). January 24, 2005. Available at www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL3163401242005.pdf. Accessed January 31, 2012.

[3] U.S. Dept. of Health and Human Services. *Standards for Privacy of Individually Identifiable Health Information*. 45 C.F.R. Parts 160, 164.

[4] Stevens GM. Congressional Research Service. *A Brief Summary of the Medical Privacy Rule* (RS20934). April 30, 2003. Available at www.law.umaryland.edu/marshall/crsreports/crsdocuments/RS20934.pdf. Accessed January 31, 2012.

[5] U.S. Dept. of Health and Human Services. "Summary of HIPAA Privacy Rule" website. Available at www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html. Accessed January 31, 2012.

This document was compiled in June–December 2011 and reflects the laws and programs current then. It reflects only portions of the laws relevant to public health emergencies and is not intended to be exhaustive of all relevant legal authority. This resource is for informational purposes only and is not intended as a substitute for professional legal or other advice. The document was funded by CDC Award No. 1U38HM000454 to the Association of State and Territorial Health Officials; Subcontractor PI Elliott, Logan Circle Policy Group LLC.