The HIPAA Privacy Rule

The HIPAA Privacy Rule *(45 C.F.R. Part 164, Subparts A, E)* established, for the first time, a set of federal standards for the protection of personal health information. Although the Health Insurance Portability and Accountability Act of 1996 *(HIPAA, P.L. 104-191)* was enacted primarily to improve the availability of health insurance coverage, it included a series of requirements under the subtitle "Administrative Simplification" to improve the efficiency of health care by supporting a transition to standardized electronic administrative and financial transactions. As part of Administrative Simplification, Congress required promulgation of privacy and security standards in recognition of the increased risk to health data posed by increased electronic data use and exchange within the health care system.

To Which Entities Does the Privacy Rule Apply?

Covered Entities

Health care providers
(who transmit any health information in electronic form in connection with a HIPAA-covered transaction)

Health care clearinghouses

Health plans

Business Associates

The rule governs business associates' use and disclosure of Protected Health Information **(PHI)**. Business associates have contractual arrangements—business associate agreements—to perform certain work on behalf of covered entities that requires disclosure and use of PHI.

Claims processing | **Data analysis** | **Utilization review** | **Billing**

What Information Does the Privacy Rule Govern?

The rule governs protected health information. PHI is individually identifiable health information **(IIHI)** that is transmitted or maintained by any form or medium. IIHI is health information that **(1)** identifies an individual: **(2)** is created or received by a covered entity or an employer, and **(3)** "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." Exceptions to PHI include, for example, certain education and employment records.

PHI May Include

- **Demographic data** *(e.g., name, social security number)*
- **Prescriptions**
- **Family health history**
- **Blood test results**
- **Imaging exams**
- **Vaccination status**

Deidentified PHI

The rule does not apply to deidentified PHI held by a covered entity, and it specifies two methods for deidentification:

- expert determination, where an expert documents that there is a small risk that the information could be used to identify the subject of the information, or
- safe harbor, where the data are stripped of 18 specific identifiers *(e.g., phone number, email address)*.

HIPAA Privacy Rule Requirements

Use and Disclosure Requirements

The rule prohibits a covered entity from using or disclosing PHI except as expressly permitted or required. For all uses or disclosures of PHI that are not otherwise permitted or required by the rule, covered entities must obtain a patient's written authorization.

Administrative Requirements

The rule requires covered entities to put in place safeguards to protect PHI from unauthorized access, use, or disclosure.

Individual Rights of Access

The rule gives individuals certain rights of access with respect to their own health information *(e.g., amendment)*.

Permissible Uses and Disclosures

In general, covered entities may between and among themselves use or disclose PHI for the purposes of treatment, payment, and other routine health care operations without patient authorization.

For disclosures to family members and friends and from public directories maintained by certain facilities, covered entities must give the individual an opportunity to object or agree to the disclosure.

The rule permits a covered entity to disclose PHI to noncovered entities, without written authorization or the opportunity to agree or object, for 12 public interest or national priority purposes *(e.g., as required by law, for public health activities, for health oversight, for law enforcement, or for judicial and administrative proceedings)*.

Information as of November 18, 2024. Prepared by Amanda Sarata, Specialist in Health Policy, and Brion Long, Visual Information Specialist.

CRS

Author Information

Amanda K. Sarata
Specialist in Health Policy

Disclaimer