



---

WRIGHT B. LAUTEN, M.D.  
MARTIN L. THOMLEY, M.D.  
HATTIESBURG - MERIDIAN - COLUMBUS  
P: (601) 255-0736 F: (601) 255-0735

---

## **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

## **HIPAA Privacy Rule**

The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.

## **Covered Entities**

The following types of individuals and organizations are subject to the Privacy Rule and considered covered entities:

- *Healthcare providers*: Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has established standards under the HIPAA Transactions Rule.
- *Health plans*: Entities that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans.
  - Exception: A group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.
- *Healthcare clearinghouses*: Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.
- *Business associates*: A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include claims processing, data analysis, utilization review, and billing.

## Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

- Disclosure to the individual (if the information is required for access or accounting of disclosures, the entity **MUST** disclose to the individual)
- Treatment, payment, and healthcare operations
- Opportunity to agree or object to the disclosure of PHI (Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object)
- Incident to an otherwise permitted use and disclosure
- Public interest and benefit activities—The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for [12 national priority purposes](#)
- [external icon](#)

1. When required by law
2. Public health activities
3. Victims of abuse or neglect or domestic violence
4. Health oversight activities
5. Judicial and administrative proceedings
6. Law enforcement
7. Functions (such as identification) concerning deceased persons
8. Cadaveric organ, eye, or tissue donation
9. Research, under certain conditions
10. To prevent or lessen a serious threat to health or safety
11. Essential government functions
12. Workers compensation
- Limited dataset for research, public health, or healthcare operations

## HIPAA Security Rule

While the HIPAA Privacy Rule safeguards protected health information (PHI), the Security Rule protects a subset of information covered by the Privacy Rule. This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called “electronic protected health information” (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

To comply with the HIPAA Security Rule, all covered entities must do the following:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information
- Detect and safeguard against anticipated threats to the security of the information
- Protect against anticipated impermissible uses or disclosures
- Certify compliance by their workforce

Covered entities should rely on professional ethics and best judgment when considering requests for these permissive uses and disclosures. The HHS Office for Civil Rights enforces HIPAA rules, and all complaints should be reported to that office. HIPAA violations may result in civil monetary or criminal penalties.

For more information, visit the Department of Health and Human Services [HIPAA website](#)



Centers for Disease Control and Prevention  
CDC 24/7 : Saving Lives, Protecting People  
Last reviewed: September 14, 2018