



Public Health Professionals Gateway

[Public Health Professionals Gateway Home](#)

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.

| | | | |
|--|--|--|--|
| FERPA The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records. The Act serves two primary purposes: 1. Give parents or eligible students more control of their educational records. 2. Prohibit educational institutions from disclosing "personally identifiable information in education records" without written consent. | Any public or private school: - Elementary - Secondary - Post secondary Any state or local education agency Any of the above must receive funds under an applicable program of the US Department of Education | Student Education Records: Records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution | • School officials • Schools to which a student is transferring • Specified officials for audit or evaluation purposes • Appropriate parties in connection with financial aid to a student • Organizations conducting certain studies for or on behalf of the school • Accrediting organizations • Appropriate officials in cases of health and safety emergencies • State and local authorities, within a juvenile justice system, pursuant to specific state law • To comply with a judicial order or healthily issued subpoena |
| HIPAA The Health Insurance Portability and Accountability Act (HIPAA) is a national standard that protects sensitive patient health information from being disclosed without the patient's consent or knowledge. Via the Privacy Rule, the main goal 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. | Every healthcare provider who electronically transmits health information in connection with certain transactions • Health plans • Healthcare clearinghouses • Business associates that act on behalf of a covered entity, including claims processing, data analysis, utilization review, and billing | Protected Health Information: Individually identifiable health information that is transmitted or maintained in any form or medium electronic, oral, or paper by a covered entity or its business associates, including certain educational and employment records | • To the individual • Treatment, payment, and healthcare operations • Uses and disclosures with opportunity to agree or object by adding the individual or giving opportunity to agree or object • Incident to an otherwise permitted use and disclosure • Public interest and benefit activities (e.g., public health activities, activities of abuse or neglect, accidents, research, law enforcement purposes, unless those to health and safety) • Limited datasets for the purposes of research, public health, or healthcare operations |

[Compare HIPAA with FERPA](#)

HIPAA Privacy Rule

The Privacy Rule standards address the use and disclosure of individuals' health information (known as *protected health information* or *PHI*) 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 make sure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public's health and well-being. The Privacy Rule 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
 - Other transactions for which HHS has established standards under the HIPAA Transactions Rule.
- **Health plans:**
Health plans include:


- Health, dental, vision, and prescription drug insurers
- Health maintenance organizations (HMOs)
- Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers
- Long-term care insurers (excluding nursing home fixed-indemnity policies)
- Employer-sponsored group health plans
- Government- and church-sponsored health plans
- 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
 - Billing

Permitted Uses and Disclosures

The law permits, but does not require, a covered entity to use and disclose PHI, 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
 - An entity can obtain informal permission 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
- Limited dataset for research, public health, or healthcare operations
- Public interest and benefit activities—The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for [12 national priority purposes](#)  :

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

HIPAA Security Rule

While the HIPAA Privacy Rule safeguards 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*, or *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:

- Ensure the confidentiality, integrity, and availability of all e-PHI
- Detect and safeguard against anticipated threats to the security of the information
- Protect against anticipated impermissible uses or disclosures that are not allowed by the rule
- 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 HHS's [HIPAA website](#).

Additional Resource

[HIPAA Enforcement](#). US Department of Health and Human Services.

Page last reviewed: June 27, 2022