

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Definitions

Authorization- written permission from the individual to the covered entity, which allows use and disclosure of PHI for purposes other than treatment, payment, and health care operations (45 CFR, section 164.506).

Authorizations require certain core elements to be included.

Authorizations must include a description of the information to be used or disclosed, with sufficient specificity to allow the covered entity to know which information the authorization references. There are no limitations on the information that can be authorized, though HIPAA stresses the importance of requesting or submitting the *minimally necessary* amount of information required to fulfill the record request. It must include the name or specific identification of the person(s) or class of persons that are authorized to use or disclose the protected health information. It must also include to whom the covered entity is authorized to make the use or disclosure. It must state an expiration date or event (specific date or specific time period). It must also state that the individual has the right to revoke the authorization in writing. It must inform the individual that when the information is used or disclosed pursuant to the authorization it may be subject to re-disclosure by the recipient and may no longer be protected by this rule. It must also include the individual's signature and the date of the signature (45 CFR, section 164.506c). An example from 45 CFR, section 164.506a states, *when a covered provider asks the individual for written permission to obtain the individual's medical record from another provider for treatment purposes, it must do so with an "authorization", not a "consent"*.

Business Associates- An organization performing an activity or function on behalf of, or providing a service to, the Covered Entity will have access to, or receive, protected health information. Basically, if you send data that identifies patients to another company, then that company is a business associate of yours. If you receive data from somebody else, you would be their business associate. Written agreements between covered entities and business associates may need to be implemented with assurances that the information will be used for certain purposes only and will be protected from disclosure by the recipient.

Consent - a consent allows use and disclosure of protected health information only for treatment, payment, and health care operations. It is written in general terms and it allows use and disclosure of protected health information by the covered entity seeking the consent, not by other persons. It is required for covered health care providers to obtain the individual's consent prior to using or disclosing PHI to carry out treatment, payment or health care operations (45 CFR, section 164.506 and 164.506a).

Covered Entities- any health care providers, health plans, or clearinghouses that electronically transmit medical information such as billing, claims, enrollment, or eligibility verification must meet HIPAA guidelines. Covered entities also include medical practices, employers, rehabilitation centers, nursing homes, public health authorities, life insurance agencies, billing agencies, and some vendors, service organizations, and universities.

Education Records - directly relate to a student and are maintained by an educational agency or institution or be a party acting for the agency or institution. They are not considered protected health information because they fall under the protection of FERPA. They do not include records of a student who is 18 years of age or older, or is attending an institution of postsecondary education that are:

1. Made by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in their capacity.
2. Made, maintained, or used only in connection with treatment of the student; and
3. Disclosed only to individuals providing the treatment.

FERPA (Family Educational Rights and Privacy Act) - it is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 making them an "eligible student".

1. Parents or eligible students have the right to inspect and review the student's education records maintained by the school.
2. Parents or eligible students have the right to request that the school correct records, which they believe to be inaccurate or misleading.

Generally, schools must have written permission from the parent or eligible student in order to release any information from the student's education record. However, FERPA allows schools to disclose those records without consent to the following parties or under following conditions (34 CFR, section 99.31):

1. School officials with legitimate educational interest;
 2. Other schools to which a student is transferring;
 3. Specified officials for audits or evaluation purposes;
 4. Appropriate parties in connection with financial aid to a student;
 5. Accrediting organizations;
 6. To comply with a judicial order or lawfully issued subpoena;
 7. Appropriate officials in case of health and safety emergencies;
- and

8. State and local authorities, with a juvenile justice system pursuant to State Law.

HIPAA (Health Insurance Portability and Accountability Act of 1996) - 45

CFR notes three major purposes for this regulation:

1. To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;
2. To improve the quality of health care in the U.S. by restoring trust in health care systems among consumers; and
3. To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection, that builds on efforts by states, health systems, and individual organizations and individuals.

Regarding privacy provisions, it prohibits health care providers, health plans, and health care clearinghouses from using or disclosing individually identifiable information except as authorized by the patient or as otherwise permitted by the regulation.

Minimum Necessary – This refers to a limit of the amount of information included in transactions in order to complete a task or fulfill a record request. The use, disclosure, or request must include the minimum amount of necessary PHI needed by the agency. Agencies need to be specific when requesting PHI from other agencies.

Privacy Notice – HIPAA states that an individual must be given adequate notice of the uses or disclosures of protected health information (PHI) that may be made by the covered entity and of the individual's rights, and the covered entity's duties, with respect to PHI (45 CFR 164.520). There are 8 required elements that need to be included in this notice:

1. ***Specific Statement*** - Specific wording for header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY".
2. ***Descriptions*** – must indicate the types of uses and disclosures the covered entity is permitted to make for treatment, payment, or operations (TPO) purposes.
3. ***Certain uses/disclosures*** – if the covered entity intends to engage in the following activities, the notice must contain a separate statement that:
 - a. The covered entity may contact the individual for appointment reminders;
 - b. The covered entity may contact the individual to raise funds for the covered entity; or

- c. A group health plan, or health insurance issuer or HMO with respect to the group health plan, may disclose PHI to the plan sponsor.
4. ***Individual's rights*** – must give statement of the individual's rights regarding PHI and a description of how to exercise those rights.
5. ***Covered Entity's Duties*** – statement that the covered entity is required to maintain privacy, that they are to abide by the notice, and a statement that relates to how the covered entity reserves the right to change the privacy notice as long as they indicate how the revised notice can be made available.
6. ***Complaints*** – How and to whom the individual can voice a complaint.
7. ***Contact*** – Name or title and telephone number of a person or office to contact for further information relating to the privacy notice.
8. ***Effective date*** – first effective date of the notice must be included, but must not be earlier than the date the notice is printed or otherwise published.

Protected Health Information (PHI) - medical information that contains any of a number of patient identifiers including name, Social Security number, telephone number, medical record number or ZIP code. The regulation protects all individually identifiable health information in any form (electronic, paper-based, oral) that is stored or transmitted by a covered entity. The definition in the rule retains the exception relating to individually identifiable information in “education records” governed by FERPA.

Treatment, Payment, and Health Care Operations (TPO) - as defined by the Privacy Rule at 45 CFR, section 164.501:

1. “Treatment” generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
2. “Payment” encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan and to obtain or provide reimbursement for the provision of healthcare.
3. “Health care operations” are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.