

One of the main aims of HIPAA is to protect the privacy of patients by ensuring certain types of information are safeguarded and not disclosed to unauthorized individuals, but what information is protected under HIPAA law?

What Information is Protected Under HIPAA Law?

Health Insurance Portability and Accountability Act (HIPAA) law was passed in 1996, it is a federal law that sets a national standard to protect all individually identifiable health information that is held by or transmitted by a HIPAA covered entity or business associate. According to the Department of Health and Human Services' Office for Civil Rights there are 18 identifiers that make health information personally identifiable. When these data elements are included in a data set, the information is considered protected health information and subject to the requirements of the HIPAA Privacy, Security and Breach Notification Rules.

The following information is protected under HIPAA law:

1. Names
2. Addresses (including subdivisions smaller than state such as street, city, county, and zip code)
3. Dates (except years) directly related to an individual, such as birthdays, admission/discharge dates, death dates, and exact ages of individuals older than 89
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate and license numbers
12. Vehicle identifiers
13. Device identifiers and serial numbers
14. Website URLs
15. IP addresses
16. Biometric identifiers, including fingerprints, voice prints, iris and retina scans
17. Full-face photos and other photos that could allow a patient to be identified
18. Any other unique identifying numbers, characteristics, or codes

What are the Allowable Uses and Disclosures of Protected Health Information?

Ensuring policies and procedures are developed and implemented to restrict the uses and disclosures of Protected Health Information (PHI) is an important element of HIPAA compliance. If health information is used for purposes not permitted by the HIPAA Privacy Rule or is deliberately disclosed to individuals unauthorized to receive the information, there are possible penalties for the covered entity or individual responsible.

HIPAA permits protected health information to be used for healthcare operations, treatment purposes, and in connection with payment for healthcare services. Information may be disclosed to third parties for those purposes, provided an appropriate relationship exists between the disclosing covered entity and the recipient covered entity or business associate. A covered entity can only share PHI with another covered entity if the recipient has previously or currently has a treatment relationship with the patient and the PHI relates to that relationship. In the case of a disclosure to a business associate, a business associate agreement must have been obtained. In all cases, the minimum necessary standard applies. Disclosures must be restricted to the minimum necessary information that will allow the recipient to accomplish the intended purpose of use.

Does HIPAA Prohibit All Other Uses of PHI?

HIPAA does not prohibit the use of PHI for all other purposes. PHI can be used for marketing purposes, can be provided to research organizations, and can even be sold by a healthcare organization. However, prior to any use or disclosure of health information that is not expressly permitted by the HIPAA Privacy Rule, one of two steps must be taken:

1. A HIPAA authorization must be obtained from a patient, in writing, permitting the covered entity or business associate to use the data for a specific purpose not otherwise permitted under HIPAA.
2. The health information must be stripped of all information that allow a patient to be identified.