Patient privacy: HIPAA basics

The **Health Insurance Portability and Accountability Act** of 1996 (**HIPAA**) is a series of national standards that health care organizations must have in place to safeguard the privacy and security of patients' health data, in all forms. It defines and covers **protected health information (PHI)**, which includes any demographic individually identifiable information that can be used to identify a patient, such as name, address, phone number, and facial photos.

Every health care provider, regardless of size, who electronically transmits any health information is considered to be a **covered entity (CE)** and must comply with HIPAA policies.

HIPAA has two main parts. The **HIPAA Privacy Rule** sets national standards for the privacy, integrity, and availability of PHI. The rule outlines safeguards that must be in place to ensure that PHI is kept private. The Rule also establishes guidelines for patients' rights to access their medical records, in addition to uses, disclosures, and authorizations that CEs must have in place. The Privacy Rule applies to all forms of PHI – electronic, written or oral.

The **HIPAA Security Rule** sets national standards for maintaining the security of PHI through a series of technical, physical, and administrative safeguards.

HIPAA protects all information about patient care, including:

- All information in a patient's medical record
- Conversations the health care provider has about the patient's care or treatment
- Information about the patient in the insurer's and provider's computer systems
- Billing information and most other patient information kept by covered entities

What is the responsibility of the covered entity?

- The covered entity must have safeguards to protect patients' PHI.
- The covered entity must reasonably limit uses and disclosures.
- The covered entity must ensure that their contractors appropriately safeguard PHI.
- The covered entity must have procedures in place to limit who can view and access PHI.
- The covered entity must implement training programs for employees, volunteers, and interns about protecting PHI.

Who can look at or receive a patient's PHI?

Health information is protected in a way that does not interfere with patient health care.
It can be used or shared:

- For patient treatment and care coordination
- To pay health care providers for patient health care and to help run CE businesses
- With relatives, friends, or others patient identifies who are involved with patient's health care or health care bills, unless the patient objects
- To make sure health care providers give quality care
- To make required reports to the police (for example, if abuse is suspected)

Unless specifically allowed by HIPAA, Private Health Information (PHI) cannot be used or shared without the patient's written permission. Without patient authorization, covered entities generally cannot:

- Give PHI to the patient's employer
- Use or share PHI for marketing or advertising purposes
- Share private notes about patient's health care

What rights do patients have over their PHI?

Health insurers and providers who are covered entities must comply with a patient's right to:

- Ask to see and get a copy of their health records
- Have corrections made to their health information
- Receive a notice describing how their PHI may be used and shared
- Decide whether to give permission to share PHI for certain purposes, such as marketing
- Get a report on when and why their PHI was shared for certain purposes

If a patient believes their rights are being denied or their PHI isn't protected, they have the right to file complaints with the provider or with the federal government.