



HIPAA

Why Do We Need to Know the Privacy Rule?

As Clinicians, professionals, and representatives of a highly valued organization we need to ensure we protect sensitive personal and health information. Establishing and practicing safeguards encompasses our values of quality and ethics.

The HIPAA Privacy Rule was enacted to protect an individuals' medical records and personal health information. These standards apply to covered entities (health plans, health care clearinghouses, and health care providers that conduct certain electronic health care transactions).

The Basic Principle of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may only use or disclose protected health information: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

What information do we have to protect?

Protected Health Information (PHI) is protected by law and is any information that can be used to identify the past, present, or future healthcare of an individual or payment for that care. The Privacy Rule protects all "individually identifiable health information" stored or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

It is our responsibility to protect "individually identifiable health information" including demographic data, that relates to the following:

- the individual's past, present or future mental or physical health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual.

We also need to protect any information that identifies the individual or information that can be used to identify the individual.

An example of common identifiers are: name, address, birth date, Social Security Number, etc.

What is required and permitted to be disclosed.

Required Disclosures. A covered entity must disclose protected health information in only two conditions: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review of enforcement action.

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 conditions: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Common ways HIPAA is Breached:

- **Unsecured Records** (left out in the open, open tablets/computers)
- **Unencrypted Data**
- **Lost or Theft of Devices** (phones, tablets, computers, etc.)
- **Gossiping or Sharing PHI** (talking about patients in hallways, lunch rooms)
- **Employee Dishonesty**
- **Improper disposal of records** (recycle bins and trash bins)
- **Unauthorized Release of Information**
- **3rd Party Disclosure of PHI**

What we can do to secure and protect PHI:

- Look at a patient's records only when needed to do your job
- Ensure communications transmitted outside the Diamond Network are encrypted
- Ensure phones, tablets, computers with PHI are kept secure
- Do not gossip about patients
- Share PHI only when appropriate and needed to do your job
- Be ethical and adhere to all Privacy policies
- Dispose of records properly in only shred bins
- Only Release Information to authorized individuals
- Follow Privacy rules for 3rd Party Disclosures of PHI