

The HIPAA Privacy Rule mandates that private health information only be used for treatment purposes, to obtain payment for services, for healthcare operations, and for research.



HEALTH INDUSTRY DISTRIBUTORS ASSOCIATION

Serving Medical Products Distributors Since 1902

HIPAA PRIVACY BASICS

ALL PROVIDERS NEED TO KNOW ABOUT PRIVACY REGULATIONS

The HIPAA Privacy Rule establishes safeguards to protect patient health information (PHI), enables patients to find out how their information is used and how to control disclosures, limits the release of PHI to the minimum needed, and gives patients the right to obtain a copy of their health records.

In order to accomplish this, the Privacy Rule requires that providers inform all patients of their rights, adopt and implement privacy procedures, train employees on new protocols, appoint a compliance officer, and secure PHI so that data is inaccessible to those that don't need it.

Incidental Disclosures

HIPAA does allow for incidental disclosures of PHI. For example, a hospital visitor may overhear a provider's conversation or may see a patient's name on a sign-in sheet. These disclosures are permissible under HIPAA only if the covered entity has applied reasonable safeguards and implemented the minimum necessary standards.

Reasonable Safeguards

Reasonable safeguards are protections that limit disclosures. HIPAA does not detail the safeguards, but it is recommended that basic "common sense" protocols are followed, including speaking quietly when discussing a patient's condition, isolating and locking file cabinets and record rooms, and providing technical security such as passwords to protect computers holding PHI.

Minimum Necessary

Minimum necessary standards require that providers limit the PHI used and disclosed, identify jobs that require access to PHI, and limit the personnel with access to PHI. If PHI is disclosed regularly to those that don't require that information, the facility is in violation of the minimum necessary standard and it will be held accountable for any disclosures.

Business Associates

HIPAA allows PHI disclosures to business associates operating on behalf of the covered entity if the information is needed to perform the job. HIPAA requires that all providers obtain contractual assurances from business associates that prevent disclosures other than for uses permitted by law. Examples of business associates include auditors, medical transcriptionists, pharmacy benefits managers, or long term care distributors providing billing services.

HIPAA PRIVACY FAQs

- **Will the Rule permit a provider to disclose a complete medical record, even though portions may have been created by others?**

Yes, if the disclosure is for treatment or payment.

- **Can a physician fax PHI to another provider?**

Yes, if providers have appropriate safeguards in place. For example, confirming the fax number and placing fax machines in secure locations.

- **Can facilities use sign-in sheets or call out the names of patients?**

Yes. The identity of the patient can be disclosed as long as the sign-in sheet, etc. does not disclose medical information or ask the patient to describe a medical condition.

- **Is it legal for a clinic to put patient charts outside an exam room?**

Yes. The purpose of leaving the chart outside the exam room is to provide the key medical information, so the minimum necessary requirement is satisfied. Providers should safeguard the chart by limiting access to exam areas, ensuring that the area is supervised, escorting non-employees in the area, and/or facing the chart to the wall.

- **Can a hospital display patient names next to the rooms they occupy?**

Yes, if the disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or for operations purposes (for example, as a service for patients and their families). In this case, the disclosure of names is the minimum necessary, and there aren't additional safeguards that would be reasonable in these circumstances.

- **Many hospitals maintain patient directories. Is this a violation?**

No, as long as information is limited to the individual's name, room number, general health condition, and religious affiliation. The facility may disclose this information to clergy (with permission from the patient) and those who ask for the individual by name.

- **How do liability insurers continue to arrange for and maintain policies for providers under the Rule?**

A provider may disclose PHI to a liability insurer, as this is essential for health care operations.

- **Does the Rule permit covered entities or collection agencies to obtain payment from parties other than the patient, e.g., spouses or guardians?**

Yes, the Rule does not limit to whom disclosures may be made in order to obtain payment. However, the covered entity or business associate must limit the amount of PHI disclosed to the minimum necessary, and abide by any requests for confidentiality and any contracted terms regarding use of PHI.

- **Are providers considered business associates of a health plan or payer?**

Generally, no. But, a business associate relationship could arise if the provider is performing a function on behalf of the health plan (e.g., case management services).

- **Do covered entities need to monitor their business associates?**

No. However, if a covered entity discovers a violation of the contract, it must act to end the violation, and, if unsuccessful, to terminate the contract with the business associate. If termination is not feasible, the covered entity must report the problem to the Office of Civil Rights.

- **Should covered entities have business associate contracts with repairmen or janitors?**

No, those that do not require access to PHI to perform their jobs do not meet the definition of a business associate. If a service is hired to do work where disclosure of PHI is not limited (such as routine handling of records or shredding of documents containing PHI), it is considered a business associate.

- **Is a medical products distributor considered a business associate?**

Generally, no. Distributors are business associates only if they require PHI to perform their jobs, as is the case with those that bill patients on behalf of the covered entity.

- **Are the U.S. Postal Service, UPS, and delivery employees business associates?**

No. These organizations act as conduits for PHI. Since no disclosure is intended by the covered entity and the probability of exposure is very small, they are not business associates.

- **Are long/short term disability, workers compensation, and automobile liability insurance plans considered covered entities?**

No.

- **Are third party administrators to a group health plan covered entities?**

No, but they generally are considered business associates.

- **Is the Privacy Rule compliance date delayed by the Administrative Simplification Compliance Act (ASCA)?**

No, the compliance date for the Privacy Rule is April 14, 2003. ASCA delays compliance with the Transaction and Code Set standards.