



Understanding HIPAA: Your Medical Privacy Rights

What Every Patient Should Know About Accessing, Protecting, and Sharing Medical Information

What Is HIPAA, and Why Does It Matter?

When you visit a physician, undergo medical testing, or receive treatment at a hospital, you share information that is among the most personal details of your life. Your medical records may contain diagnoses, prescriptions, laboratory results, financial information, and details about your physical and mental health. Naturally, you expect that information to remain confidential.

The Health Insurance Portability and Accountability Act (HIPAA), enacted by Congress in 1996, established the foundation for federal protections governing medical information. Subsequent regulations, particularly the HIPAA Privacy Rule and Security Rule, created national standards for protecting health information and regulating its use and disclosure.

HIPAA does more than require healthcare organizations to safeguard patient information. It also gives patients important rights to examine their medical records, obtain copies, request corrections, and exercise certain controls over how their information is shared. Understanding those rights can help patients become more informed participants in their own healthcare.

Who Must Comply with HIPAA?

HIPAA applies primarily to organizations known as *covered entities*. These include health insurance plans, healthcare clearinghouses, and healthcare providers that conduct certain standard administrative transactions electronically. Hospitals, physicians, pharmacies, and many other healthcare organizations generally fall within these categories.

The law also applies to *business associates*, organizations or individuals that handle protected health information while performing services for covered entities. Examples include medical billing companies, certain technology vendors, and contractors that maintain electronic patient records. These businesses have their own legal obligations to protect the information entrusted to them.

However, HIPAA does not apply to everyone who possesses medical information. Employers, fitness applications, and consumer health websites are not automatically covered merely because they collect health-related data. Other federal and state privacy laws may govern their activities.

Your Right to Examine and Obtain Medical Records

One of HIPAA's most important protections is the right to inspect and obtain copies of medical and billing records maintained by covered healthcare organizations. These records may include physician notes, laboratory results, diagnostic images, prescriptions, insurance information, and other materials used to make decisions about your care.

Patients can generally request their records in paper or electronic form. When information is readily available electronically, HIPAA provides rights concerning the requested format, subject to applicable requirements and technical capabilities. Providers ordinarily must respond within 30 calendar days, although a single extension of up to 30 additional days may be permitted with proper written notice.

A healthcare provider cannot refuse access simply because a patient has an unpaid medical bill. Providers may charge certain reasonable, cost-based fees for copies, but HIPAA generally prohibits charging for searching for or retrieving records. The right to obtain medical information does not depend on whether the patient has satisfied an outstanding financial obligation.

Can You Correct Mistakes in Your Medical Records?

Medical records are not always accurate. A patient's file may contain an incorrect medication, an outdated diagnosis, a mistaken date, or information entered into the wrong chart. Such errors can affect future treatment, insurance decisions, and communication among healthcare providers.

HIPAA gives patients the right to request amendments to protected health information in designated record sets. A provider generally must respond within 60 days, with a possible 30-day extension when the required conditions are met.

The provider is not required to accept every requested correction. For example, a physician may disagree with a patient's interpretation of a diagnosis or determine that the existing record is accurate. When an amendment is denied, patients generally have the right to submit a written statement of disagreement that becomes associated with the disputed information.

Who Can See Your Medical Information?

HIPAA restricts how covered organizations use and disclose protected health information, but it does not require written permission for every disclosure. Healthcare providers may generally share relevant information for treatment, payment, and healthcare operations without obtaining a separate patient authorization.

For example, your primary care physician may send medical records to a specialist involved in your treatment. A hospital may provide necessary billing information to your health insurance company, and a healthcare organization may use certain records for quality improvement and administrative purposes.

Other disclosures are permitted or required under specific circumstances, including certain public health activities, law enforcement purposes, and legally mandated reporting. HIPAA establishes conditions and limitations for these disclosures rather than imposing an absolute prohibition on sharing medical information.

For many purposes unrelated to treatment, payment, or healthcare operations, specific authorization may be required. HIPAA generally restricts the sale of protected health information without authorization and imposes special rules on many marketing uses.

Can You Keep Information from Your Health Insurance Company?

Patients sometimes pay for medical services themselves because they do not want a particular treatment disclosed to their health insurance company. HIPAA provides an important protection in this situation.

When a patient pays a healthcare provider entirely out of pocket for a particular service, the patient may request that information about that service not be disclosed to a health plan for payment or healthcare operations. Subject to specified exceptions, including disclosures required by law, the provider must honor that restriction.

This protection is narrower than a general right to prevent all sharing of medical information. It applies under particular circumstances and does not necessarily prevent disclosures for other legally permitted purposes.

Medical Privacy and Older Americans

HIPAA is especially important for older adults who rely on spouses, adult children, relatives, or caregivers to help manage their medical needs. Families sometimes assume that privacy laws prevent physicians from discussing a parent's condition with an adult child, even when the parent wants that involvement.

Fortunately, HIPAA provides considerable flexibility. When a patient agrees, has an opportunity to object but does not, or when the circumstances reasonably indicate agreement, healthcare professionals may share relevant information with family members and others involved in the patient's care or payment for care.

If a patient is incapacitated or unavailable, a healthcare professional may disclose relevant information when, using professional judgment, the disclosure is in the patient's best interests. Such disclosures should generally be limited to information directly related to the person's involvement in the patient's care.

A patient may also designate a personal representative through legally recognized authority, such as an appropriate healthcare power of attorney. Because state laws determine many aspects of that authority, families should consider preparing the necessary documents before a medical emergency occurs.

What About Psychotherapy Notes?

HIPAA provides special protections for certain psychotherapy notes maintained separately from a patient's ordinary medical record. These are notes recorded by a mental health professional documenting or analyzing conversations during counseling sessions.

Such notes are generally excluded from the patient's HIPAA right of access, and their disclosure ordinarily requires specific authorization unless an exception applies. However, this exclusion does not extend to all mental health information. Diagnoses, medication records, treatment plans, progress notes, and other information maintained in the regular medical record generally remain subject to ordinary access rules.

The distinction is important because patients should not assume that every document involving mental healthcare is inaccessible. HIPAA protects the confidentiality of sensitive counseling notes while preserving patients' rights concerning most other mental health records.

HIPAA and Assisted Living Facilities

Medical privacy concerns frequently arise in assisted living communities, nursing homes, and other residential care settings. Residents may receive medications, medical treatment, personal assistance, and other services involving sensitive health information.

Whether HIPAA applies directly to a particular assisted living facility depends on its operations and whether it qualifies as a covered entity or business associate. Nursing homes and other

healthcare providers may be covered when they meet the law's requirements, but not every residential facility is automatically subject to HIPAA.

Even when HIPAA does not apply directly, state privacy laws, licensing requirements, and professional confidentiality obligations may protect residents' information. Residents themselves are generally free to discuss their own medical conditions with neighbors, friends, or family members if they choose.

What Happens When HIPAA Is Violated?

Healthcare organizations must implement appropriate safeguards to protect patient information. Depending on the circumstances, these may include employee training, secure computer systems, access controls, encryption, physical security, and procedures for responding to suspected breaches.

Federal regulators have investigated organizations following incidents involving stolen computers, improperly disclosed records, cybersecurity failures, and inadequate protection of electronic health information. Enforcement actions may result in corrective action plans, financial settlements, or civil monetary penalties, depending on the nature and seriousness of the violations.

Not every accidental disclosure constitutes a punishable violation, and HIPAA does not guarantee that unauthorized access can never occur. The law requires covered organizations to comply with applicable privacy and security obligations and respond appropriately when protected information is compromised.

How to File a HIPAA Complaint

Patients who believe their medical privacy rights have been violated may file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights (OCR). Complaints can be submitted electronically or in writing and generally must be filed within 180 days of when the individual knew the act or omission occurred, although OCR may extend that period for good cause.

A complaint should describe what happened, identify the organization involved, and explain why the individual believes HIPAA requirements were violated. Patients may also raise concerns directly with the healthcare organization's privacy officer.

HIPAA prohibits covered organizations from retaliating against individuals for exercising their rights or filing complaints. However, HIPAA generally does not provide patients with a private federal lawsuit for damages solely because the statute was violated. Other legal remedies may be available under applicable state or federal laws.

The Bottom Line: Your Information, Your Rights

HIPAA establishes an important balance between medical privacy and the practical need to share

information for effective healthcare. Physicians, hospitals, insurers, and other covered organizations must protect patient information while ensuring that necessary medical communication can continue.

Patients, meanwhile, have enforceable rights to access medical records, request corrections, obtain information about privacy practices, and challenge certain unauthorized disclosures. Understanding these protections is particularly valuable for older Americans and families managing complicated healthcare arrangements.

Medical information may be maintained by healthcare providers, but patients have important rights concerning how that information is accessed, protected, and shared. Knowing those rights is the first step toward exercising them.

See Also: HIPAA and Patient Privacy

- **U.S. Department of Health and Human Services:** [Your Rights Under HIPAA](#) — An overview of patient privacy protections and access rights.
- **HHS Office for Civil Rights:** [Access to Medical Records](#) — Explains how patients can inspect, obtain, and request corrections to their medical records.
- **HHS:** [Sharing Health Information with Family Members and Friends](#) — Explains when healthcare providers may discuss medical information with relatives and caregivers.
- **HHS Office for Civil Rights:** [Filing a HIPAA Complaint](#) — Instructions for reporting suspected privacy violations.

Legal Information Notice: This article provides general educational information about HIPAA and patient privacy rights in the United States. It is not legal advice. Federal regulations, state privacy laws, and individual circumstances may affect how these protections apply.