



Your Rights (HIPAA)

HIPAA advisory

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996 to address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system.

HIPAA is the commonly accepted nickname for the Health Insurance Portability and Accountability Act of 1996. This sweeping body of legislation led to dramatic changes in virtually every administrative practice of the U.S. health care industry.

Specifically, the law assigned the U.S. Department of Health and Human Services (HHS) to develop, introduce, and enforce a new system of rules to govern accountability and standards for patient information in the Internet age.

HIPAA was signed into law on August 21, 1996. To give all parties time to comply with the new guidelines, however, the law contained a schedule for taking effect in gradual phases spread over the next decade. Most health care and insurance providers had until April 2003 or 2004 to establish compliance with HIPAA's main regulations. And some requirements remain open-ended as to when and how they will take effect.

The primary motivation for the new law was to streamline health care processes by establishing standards for electronic technology to transfer and process billing and health insurance transactions. At the same time, however, many legislators saw advances in electronic technology as a risk to the privacy of patient health information. Therefore, the law included a deadline of three years, until August 1999, for Congress to develop a corresponding privacy policy to ensure that personal information received adequate protection from criminal or commercial misuse.

If Congress failed to produce a suitable privacy policy by that date, the law instructed Health and Human Services (HHS) to step in and develop a suitable privacy policy. In August 1999, Congress missed the self-imposed deadline, so responsibility for privacy regulations fell to HHS.

HHS published a set of tentative privacy guidelines in November 1999 and asked the legislature and the public for comments on the draft. More than 52,000 comments arrived in response and were used to revise and amend the working privacy policy.

About a year later, in December 2000, HHS published a final regulation that included rules for protecting the privacy of "Individually Identifiable Health Information." This new body of law was incorporated into the existing HIPAA and came to be known collectively as the Privacy Rule.

HIPAA's Definition of "Covered Entity"

An individual or company whose work in a health-related field requires compliance with HIPAA requirements is called a "covered entity." As defined by HIPAA, covered entities include:

- Health care providers who conduct certain transactions in electronic form;
- Health care clearinghouses; and
- Health plans (defined as almost any party that pays medical costs, such as insurance companies, HMOs, employer-sponsored group health plans, Medicare/Medicaid, etc.)

Clinical laboratories affiliated with a health care provider or other "covered entity" are subject to HIPAA and thus required by law to provide patient access to their laboratory records. If a laboratory is not affiliated with a covered entity, then state laws for patient access apply instead of HIPAA.

In California, for example, clinical laboratories not directly affiliated with health care providers are not subject to state disclosure laws; this was an intentional exclusion by the legislature to protect patients from lay misinterpretation of raw test data. California access laws require a physician who orders a laboratory test to be the person who reports the test results to a patient [CA Health & Safety Code Section 123148]. However, these test results must be recorded by the physician in the patient's records -- and, if requested by the patient under HIPAA, they must be reported in plain language within a reasonable time.

The Privacy Rule Explained

The HIPAA Privacy Rule embodied the first comprehensive federal protection for the privacy of patient health information. The regulations introduced in 2000 were modified in August 2002 to balance the patient's privacy rights with the provider's ability to provide effective medical treatment; that is, "to improve workability and avoid unintended consequences that could have impeded patient access to delivery of quality health care."

The Privacy Rule is federal law and supersedes any state laws that are less "pro-consumer." State civil laws that offer greater rights or protection for consumers than the Privacy Rule remain in effect. For example, a health care provider, Peoplechart, or any entity must comply with California laws governing disclosure and handling of medical information, because these state laws are more restrictive of disclosure and more protective of patient privacy than the HIPAA Privacy Rule.

Other areas where stricter state laws might override HIPAA could include fees charged for copying and retrieving information; time limits to respond to patient requests; and limits to situations where a provider can deny access to records.

The Office for Civil Rights (OCR), a division of HHS, is the federal agency responsible for administering and enforcing the Privacy Rule. Penalties for violations of the Privacy Rule can include fines or, in extreme cases, imprisonment. Consumer complaints should be filed with OCR within 180 days after the violation becomes known.

Your Legal Rights under the Privacy Rule

Under the terms of the HIPAA Privacy Rule:

- **Consumers have an enforceable legal right to review and copy their medical records**, based on the theory that access is the cornerstone of patient privacy policy and fair information practices. (45 CFR 164.524). Within 30 days of request, a covered entity must allow an individual to review records. If the information is not accessible onsite, the covered entity has 60 days to comply, though an extension can be given if the covered entity provides a written statement of the reasons for delay and the specific date by which it will comply.
- **Consumers have the right to amend incorrect data in their medical records** (45 CFR 164.526). Within 60 days of request, a covered entity must amend a patient's information (with limited exceptions) as indicated and provide the amendment to all entities known to have received the objectionable information. Similar to the Fair Credit Reporting Act, if a request to amend or supplement information is denied, the HIPAA Privacy Rule gives the individual the right to file a statement disagreeing with the denial, which will be included in the records.
- **Consumers have the right to an accounting of all disclosures of their personal information** to third parties by a covered entity (45 CFR 164.528).
- **Consumers have the right to a written summary of their health condition.** At the individual's request, a provider must write a summary or explanation of the individual's health condition.
- **Exceptions:** A patient may be denied access to records if a provider believes such access could endanger the physical safety of the individual or others. Also patient access may be denied for some psychotherapy notes, for information compiled for a lawsuit, or for certain other limited circumstances. All denials of patient access are subject to review and appeal.
- The content of most patient records falls within the definition of Protected Health Information (PHI).
- The Office for Civil Rights enforces compliance of the HIPAA Privacy Rule and has full responsibility for correcting and/or punishing violations.

Mandatory versus Voluntary Consent for Disclosure

In August 2002, the Privacy Rule's requirement that providers ask patients for consent to disclose any personal information was replaced with "voluntary consent" for certain functions viewed as essential to providing quality health care. Continuing to require mandatory consent for these functions was regarded as impractical and a potential impediment to delivering care.

Permission from the patient is asked or not asked at the discretion of the providers for the purposes of treatment, payment, and health care. Examples include pharmacists filling prescriptions, hospitals reviewing patient notes from a referring physician, telemedicine, and emergency medical situations. HHS inserted a cautionary note: "Although the Rule is no longer mandatory, the Rule still affords individuals the opportunity to engage in important discussions regarding the use and disclosure of their

health information through the 'strengthened notice requirement' while allowing activities that are essential to quality health care to occur unimpeded. These modifications will ensure that the Rule protects patient privacy as intended without harming consumer's access to care or to the quality of that care."

- The Privacy Rule permits a provider to disclose a complete medical record that includes portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.
- Under HIPAA, situations such as a medical emergency fall into voluntary consent, where judgment is exercised depending on the situation and provider has the option to request or not request consent for reviewing or sharing patient information.
- Federal law leaves privacy rights in medical emergencies largely under the jurisdiction of state law, which may differ as to when or where they permit disclosure of protected health information in an emergency.

Limits on Fees and Timing for Providing Patients with Access to Medical Records

- A commentary made by DHHS on the Privacy Rule disapproves of a covered entity charging a fee for the search or retrieval of a patient's requested records, though does permit reasonable per-page fee to cover the costs of photocopies and/or postage. This has not been enacted into regulations.
- This fee imposed by physicians or health care providers must not exceed any maximum cap on copying charges set by the governing state. However, for some states, the charges are not specific to the dollar and cents. As an example, Hawaii stipulates that a requesting person shall expect to bear any "reasonable costs incurred by a health care provider in making copies of medical records. Without specificity in the maximum charge, expect to pay copying fees that vary from state to state and from provider to provider within a state.
- Under California's Patient Access Laws, for example, copies of records must be "sent within 15 days of the provider's receipt of a written request, subject to copying costs of not over 25 cents per page plus reasonable clerical costs" (HSC 123110(b)).
- If the physician, health care provider organization, or health plan **does not** actually **maintain the individual's records**, but knows where the information is available, it must direct the individual to the source of his/her records.
- If the patient requests, a physician or provider must prepare a summary or explanation of the patient's health information or condition and may charge a fee for preparing this document.

HIPAA Information Resources

- **Office for Civil Rights home page** <<http://www.hhs.gov/ocr/hipaa/>>
"National Standards to Protect the Privacy of Personal Health Information" is the title of the OCR home page maintained by the U.S. Department of Health and Human Services. Here you'll find a

library of articles, pamphlets, and other resources for understanding HIPAA, as well as the full text of the law with all its extensions and amendments.

- **HIPAA and related legislation text** <<http://www.hipaadvisory.com/regs/>>
Along with a number of HIPAA-related editorial articles, this page offers the complete text of all HIPAA legislation.
- **Searchable HIPAA text** <<http://www.asksam.com/ebooks/hipaa/>>
- **The Privacy Rule and related codes** <<http://www.hhs.gov/ocr/combinedregtext.pdf>>
- **Health Privacy Project** <<http://www.healthprivacy.org>>
This non-profit watchdog group offers an excellent resource for educating the public on matters of personal privacy, particularly in regard to patient rights and HIPAA. Check out their info sheets and other excellent materials for learning about your rights as a consumer and patient.
- **HIPAA entry in Wikipedia** <<http://en.wikipedia.org/wiki/HIPAA>>
The ever-evolving online encyclopedia has a lengthy discussion of HIPAA, as well as links to a number of related information resources.
- **20 Tips for Preventing Medical Errors**

Agency for Healthcare Research and Quality

1 (800) 358-9295

Website: www.ahrq.gov

Specific Information: www.ahrq.gov/consumer/20tips.htm