

How Private Is My Medical Information?

Used with the permission of the Privacy Rights Clearinghouse
www.privacyrights.org.

[Also see our [FAQ](#) on medical privacy.]

- [What do my medical records contain? .](#)
- [What medical information is not covered by HIPAA? .](#)
- [Who has access to my medical records?](#)
- [How can I protect the privacy of my medical records?](#)
- [How do I get access to my own medical records?.](#)
- [How can I learn more about the federal privacy rule, HIPAA?.](#)
- [Electronic health records: What are the benefits and dangers for consumers](#)
- [Resources for additional information.](#)

Many people consider information about their health to be highly sensitive, deserving of the strongest protection under the law. Long-standing laws in many states and the age-old tradition of doctor-patient privilege have been the mainstay of privacy protection for decades.

Now, the federal Health Insurance Portability and Accountability Act (HIPAA) sets a national standard for privacy of health information, effective April 14, 2003. But HIPAA only applies to medical records maintained by health care providers, health plans, and health clearinghouses - and only if the facility maintains and transmits records in *electronic* form. A great deal of health-related information exists *outside* of health care facilities and the files of health plans, and thus beyond the reach of HIPAA. (PRC Fact Sheet 8a, "HIPAA Basics," www.privacyrights.org/fs/fs8a-hipaa.htm)

The extent of privacy protection given to your medical information often depends on where the records are located and the purpose for which the information was compiled. The laws that cover privacy of medical information vary by situation. And, confidentiality is likely to be lost in return for insurance coverage, an employment opportunity, your application for a government benefit, or an investigation of health and safety at your work site. In short, you may have a false sense of security. This guide provides information on medical records *not covered by the HIPAA Privacy Rule*.

What do my medical records contain?

Medical records are created when you receive treatment from a health professional such as a physician, nurse, dentist, chiropractor, or psychiatrist. Records may include your medical history, details about your lifestyle (such as smoking or involvement in high-risk sports), and family medical history.

In addition, your medical records contain laboratory test results, medications prescribed, and reports that indicate the results of operations and other medical procedures. Your records could also include the results of genetic testing used to predict your future health. And they might include information about your participation in research projects.

Information you provide on applications for disability, life or accidental insurance with private insurers or government programs can also become part of your medical file.

What medical information is not covered by HIPAA?

Medical information that is not covered by the federal privacy rule might be found in your financial records, your child's school records, and/or your employment files.

Financial records. The federal Gramm-Leach-Bliley Act (GLB) allows financial companies such as banks, brokerage houses, and insurance companies to operate as a single entity. GLB gives you the right to be notified about the information-sharing practices of financial institutions. And you must be given an opportunity to opt-out of third-party information sharing. But GLB does not keep information from being shared among affiliated companies.

Your credit card account and checking transactions are likely to include information about where you go for health care. Insurance applications and medical claims also contain health-related information. So it is possible for such medical information to be shared among affiliates of financial institutions. Such information is *not* protected by HIPAA.

Some financial companies promise extra protection for medical information. And insurance companies may be prohibited from giving information to an affiliated bank by state insurance laws. It pays to examine the privacy notices of financial institutions carefully. (Read PRC Fact Sheet 24, "Protecting Financial Privacy," www.privacyrights.org/fs/fs24-finpriv.htm.)

Education records maintained by your child's school contain vaccination histories, information about physical examination for sports, counseling for behavioral problems, and records of visits to the school nurse. Privacy of education records is under the control of the US Department of Education and the Family Educational Rights and Privacy Act (FERPA). These records are not covered by HIPAA. For more information about FERPA, visit the Department's web site at www.ed.gov/offices/OM/fpco/ferpa/index.html.

Employment records and medical information may be mingled in situations not covered by HIPAA. Your employer may be covered by the Occupational Safety and Health Act (OSHA). If so, you have the right to access your medical records gathered for your employer's OSHA responsibilities. (See the web site of the US Department of Labor for more on employee's rights under OSHA, www.osha.gov/as/opa/worker/rights.html.)

In addition, the federal Family and Medical Leave Act (FMLA) gives most workers the right to 12 weeks of unpaid leave a year for personal and family health. If FMLA leave is because of a serious illness, your employer may request a doctor's certification of the illness. But the employer cannot make you produce medical records. See the U.S. Department of Labor web site for more information on FMLA, www.dol.gov/elaws/esa/fmla/faq.asp.

If your employer is self-insured for employees' medical benefits, its handling of insurance claims and other health-related information is covered by HIPAA. In this capacity, the employer would be considered a "hybrid" entity. For more information on HIPAA involving employer group health plans and self-insurance situations, read PRC Fact Sheet 8a on "HIPAA Basics," www.privacyrights.org/fs/fs8a-hipaa.htm.

Who has access to my medical records?

Your medical information is shared by a wide range of people both in and out of the health care industry. Generally, access to your records is obtained when you agree to let others see them. In reality, you may have no choice but to agree to the sharing of your health information if you want to obtain care and qualify for insurance.

1. Insurance companies usually require you to release your records before they will issue a policy or make payment under an existing policy. This is especially true if you apply for individual health

insurance as opposed to a group health plan available through your employer.

Insurance companies are considered financial institutions under the federal GLB law. Like banks and brokerage houses, they must provide you a notice of how they gather and use your customer information. You may have the right to opt-out of sharing some information with other companies.

To learn more about GLB and the insurance privacy laws in your state, visit the web site of the National Association of Insurance Commissioners, www.naic.org/state_contacts/sid_websites.htm. Medical information gathered by an insurance company may also be shared with others through the Medical Information Bureau (see below).

2. Government agencies may request your medical records to verify claims made through Medicare, MediCal, Social Security Disability, and Workers Compensation.

3. The Medical Information Bureau (MIB) is a central database of medical information shared by insurance companies. Approximately 15 million Americans and Canadians are on file in the MIB's computers. About 600 insurance firms use the services of the MIB primarily to obtain information about life insurance and individual health insurance policy applicants. When you apply for life or health insurance as an *individual*, you are likely to be asked to provide information about your health. Sometimes you are required to be examined by a doctor and/or to have your blood and urine tested. If you have medical conditions that insurance companies consider significant, the insurance company will report that information to the MIB. The information contained in a typical MIB record is limited to codes for specific medical conditions and lifestyle choices. Examples include codes to indicate high blood pressure, asthma, diabetes, or depression. A code can signify participation in high-risk sports such as skydiving. A file would also include a code to indicate that the individual smokes cigarettes. The MIB uses 230 such codes. It's important to remember the following about the MIB:

- The MIB is *not* subject to HIPAA. MIB files do *not* include the totality of one's medical records as held by your health care provider. Rather it consists of codes signifying certain health conditions.

- A decision on whether to insure you is not supposed to be based solely on the MIB report.
- The MIB is a consumer reporting agency subject to the federal Fair Credit Reporting Act (FCRA). If you are denied insurance based on an MIB report, you are entitled to certain rights under the FCRA, including the ability to obtain a free report and the right to have erroneous information corrected. See the Federal Trade Commission's web site on insurance decisions, www.ftc.gov/bcp/online/pubs/buspubs/insurers.htm.

The MIB does not have a file on everyone. But if you have an MIB file, you will want to be sure it is correct. You can obtain a copy for free once a year by calling (866) 692-6901 (TTY for the hearing impaired (866) 346-3642) or by visiting the company's web site at www.mib.com/html/request_your_record.html.

In general the MIB can be contacted at Medical Information Bureau, P.O. Box 105, Essex Station, Boston, MA 02112, or by sending an email to infoline@mib.com Web: www.mib.com.

3a. IntelliScript and MedPoint are databases that report prescription drug purchase histories to insurance companies. Like the MIB reports, IntelliScript and MedPoint reports are used primarily when consumers are seeking private health, life or disability insurance. Prescription drug databases can go back as far as five years, detailing drugs used as well as dosage and refills.

With a history of prescription drugs in hand, insurers may make assumptions about medical conditions and assess the risk of writing an insurance policy. Information in an IntelliScript or MedPoint report may prompt an insurer to deny coverage for certain conditions, increase insurance premiums, or deny coverage altogether. Such adverse actions by insurance companies trigger a sequence of consumer rights under the Fair Credit Reporting Act (FCRA).

Until recently, use of prescription drug databases was unknown to consumers. Insurers' use of these databases first came to light in 2007 when the Federal Trade Commission (FTC) sued Milliman, the owner of the IntelliScript database, and Ingenix, Inc., owner of the MedPoint database.

The FTC claimed that the companies are consumer reporting agencies subject to the FCRA. Both cases were settled without the data brokers paying a monetary penalty, but Milliman and Ingenix agreed to follow

the FCRA. This means, among other things, that consumers who apply for private insurance and are turned down because of something in an IntelliScript or MedPoint report are entitled to a copy of the report from their insurance company and an opportunity to dispute the accuracy of information in the report.

Individuals who have applied for individual health, life or disability insurance may also request a copy of any prescription report directly from MedPoint or IntelliScript. Reports are available once a year whether or not there has been an adverse decision by an insurance company.

You can request a copy of your MedPoint report by calling (888) 206-0335 or writing to: MedPoint Compliance, Ingenix, Inc., 2525 Lake Park Blvd, West Valley City Utah 84120. Additional contact information can be found at www.ingenix.com/ContactUs/

IntelliScript reports are available by calling the toll-free request line at (877) 211-4816. Consumers will have to provide their full name, date of birth, last four digits of their Social Security number and current zip code. Milliman will provide a copy of any information the company has on an individual as well as the names of insurance companies that have requested a prescription history. The company's Web site includes information about the product as well as additional contact information. www.rxhistories.com/how_it_works.html

4. Employers usually obtain medical information about their employees by asking employees to authorize disclosure of medical records. This can occur in several ways not covered by HIPAA. Unfortunately, the laws in only a few states require employers to establish procedures to keep employee medical records confidential. (For example, California Civil Code §56.)

A potential employer may ask for medical information as part of an employment background check, with limitations as explained below. To learn more on employment background checks and an employer's obligations under the FCRA, read PRC Fact Sheet 16 on background checks, www.privacyrights.org/fs/fs16-bck.htm, and the FTC's web site, www.ftc.gov/bcp/online/pubs/buspubs/credempl.htm.

According to the federal Americans with Disabilities Act in workplaces with more than 15 employees (ADA text, www.eeoc.gov/laws/ada.html, 42 USC §12101 et seq.)

- Employers may not ask job applicants about medical information or require a physical examination prior to offering employment. After employment is offered, an employer can only ask for a medical examination if it is required of all employees holding similar jobs.
- If you are turned down for work based on the results of a medical examination, the employer must prove that it is physically impossible for you to do the work required.

Report violations of the ADA to the U.S. Equal Employment Opportunity Commission (EEOC). Phone: (800) 669-4000. Web: www.eeoc.gov.

5. Your medical records may be **subpoenaed for court cases**. If you are involved in litigation, an administrative hearing, or a worker's compensation hearing and your medical condition is an issue, the *relevant* parts of your medical record may be copied and introduced in court.

6. Other disclosures of medical information occur when medical institutions such as hospitals or individual physicians are evaluated for quality of service. This evaluation is required for most hospitals to receive their licenses. Your identity may or may not be disclosed when medical practices are evaluated. Evaluations for accreditation are called "health care operations" under HIPAA. Consent to use your information for these purposes is usually not required.

Occasionally your medical information is used for health research and may be disclosed to public health agencies like the Centers for Disease Control. Specific names are usually not given to researchers. Their use of patient information is covered by HIPAA. (U.S. Dept. of Health and Human Services, www.hhs.gov, and PRC Fact Sheet 8a, www.privacyrights.org/fs/fs8a-HIPAA.htm)

7. Medical information may be passed on to **direct marketers** when you participate in informal health screenings. Tests for cholesterol levels, blood pressure, weight and physical fitness are examples of free or low-cost screenings offered to the public. Screenings are often conducted at pharmacies, health fairs, shopping malls, or other nonmedical settings. The information collected may end up in the data banks of businesses which have products to sell related to the test.

8. A tremendous amount of health-related information is found on the **Internet**. Many Usenet news groups and "chat" rooms are available

for individuals to share information on specific diseases and health conditions. Web sites dispense a wide variety of information. There is no guarantee that information you disclose in any of these forums is confidential. Always review the privacy policy of any web site you visit.

How can I protect the privacy of my medical records?

A new federal law on medical privacy, HIPAA, went into effect April 14, 2003. For the first time, federal law establishes standards for patient privacy in all 50 states, including the right of patients to access to their own records. The stronger laws already in effect in the states will not be weakened. Although HIPAA provides some protection, it is not the final answer to medical records privacy. Here are some strategies to limit others' access to your medical records:

1. When you are asked to sign a waiver for the release of your medical records, try to limit the amount of information released. Instead of signing the "blanket waiver," cross it out and write in more specific terms.

- *Example of blanket waiver:* I authorize any physician, hospital or other medical provider to release to [insurer] any information regarding my medical history, symptoms, treatment, exam results or diagnosis.
- *Edited waiver:* I authorize my records to be released from [X hospital, clinic or doctor] for the [date of treatment] as relates to [the condition treated].

2. Discuss your confidentiality concerns with your doctor. If you want a specific condition to be held in confidence by your personal physician, bring a **written request** to the appointment that revokes your consent to release medical information to the insurance company and/or to your employer for that visit. You must also pay for the visit yourself rather than obtain reimbursement from the insurance company.

To be especially certain of confidentiality, you may need to see a different physician altogether and **pay the bill yourself**, forgoing reimbursement from the insurance company. Realize that under HIPAA, your attempts to restrict the sharing of specific records can be denied by the health care provider.

3. Ask your health care provider to use caution when photocopying portions of your medical records for others. Sometimes more of your

medical records are copied than is necessary, for example, when requested by the insurance company or another health care provider.

4. Find out if your health care provider has a policy on the use of **cordless and cellular phones** and **fax machines** when discussing and transmitting medical information. Wireless telephones are not as private as standard "wireline" telephones. Because they transmit by radio wave, phone conversations can be overheard on various electronic devices. Newer digital models are more secure. (See PRC Fact Sheet 2, "Wireless Communications," www.privacyrights.org/fs/fs2-wire.htm.)

Fax machines offer far less privacy than the mail. Frequently many people in an office have access to fax transmissions. Staff members at all levels of the organization should take precautions to preserve confidentiality when sending and receiving medical documents by fax machine. (See PRC Fact Sheet 12, on responsible information-handling practices, www.privacyrights.org/fs/fs12-ih2.htm)

Your medical information is not confined to health care institutions. Here are some additional situations where you must be careful to protect your privacy.

5. If your records are **subpoenaed** for a legal proceeding, they become a public record. Ask the court to allow only a specific portion of your medical record to be seen, or better yet, not to be open at all. A judge will decide what parts, if any, of your medical record should be considered private. After the case is decided, you can also ask the judge to "seal" the court records containing your medical information.

6. If **your employer** is self-insured, the human resources department is likely to have information about any health-related claims that you file. If you are concerned about the privacy protection policies and practices of your employer, talk to the appropriate administrator. You should consider following up with a letter to the head of the department that handles health-related information. Diplomatically stress your desire for all of your health information to be handled with the utmost confidentiality. Keep a copy for yourself, filed at home.

7. Think twice before filling out **marketing-related questionnaires**. They commonly contain sections that ask for a great deal of family health information. Examples are the National Consumer Survey and the Laura David Consumer Product Survey of America. The loss of your medical privacy is a high price to pay in exchange for a few free

coupons or a chance to win a contest. For more information, read the PRC's testimony to the Federal Trade Commission in 2001, www.privacyrights.org/ar/ftc-info_mktpl.htm.

8. Before participating in **health screenings** offered in shopping malls and other public places, find out what uses will be made of the medical information that is collected. If you are not given the opportunity to say "no" to the sharing of your medical information with others, don't participate.

9. Use caution when visiting **health-related web sites** and when participating in online discussion groups.

- Carefully read the privacy policies and terms of services of medical web sites. Do not fill out registration forms unless you are satisfied with the web operator's privacy policy.
- Use a pseudonym when participating in chat rooms and online forums.
- Before sharing personal information with a health web site, find out if it participates in a web seal program such as TRUSTe, www.truste.org, URAC Health Web Site Accreditation, <http://webapps.urac.org/websiteaccreditation/default.htm>, HON (Health on the Net), www.hon.ch, and BBBOnline, www.bbbonline.org.
- Remember, companies can change their privacy policies at any time. And if the company goes bankrupt, its data base of user information could be sold to the highest bidder.

10. Establish your own history of treatment. If you decide to change physicians or health care organizations, it is a good idea to obtain copies of your medical records. Physicians may retire, move out of state or merge practices with other physicians. Health care facilities may merge with another facility or even go out of business following bankruptcy. Get copies of medical records while you can. Don't count on your ability to get your records years after treatment. If your doctor or health care provider goes out of business, be sure to find out where they intend to store the medical records of their patients.

How do I get access to my own medical records?

HIPAA requires health care providers, health plans, and health care clearinghouse to allow you access to your medical records. Notices you receive from providers and plans must include information about how you can obtain copies of your medical records.

In addition to HIPAA, about half the states have laws that allow patients or their designated representatives to access medical records. Laws usually allow health care facilities to charge a "reasonable" fee for copying records.

If you receive care in a federal medical facility, you have a right to obtain your records under the federal Privacy Act of 1974 (5 USC sec. 552a, www.usdoj.gov/foia/privstat.htm)

We advise that you make your request in writing. For a sample letter, see www.privacyrights.org/Letters/medical2.htm. If you are denied access, you can file a complaint with the U.S. Department of Health and Human Service's Office of Civil Rights. (Contact information is provided at the end of this guide). Your state's medical privacy law might also enable you to file a complaint with state regulators.

How can I learn more about the federal privacy rule, HIPAA?

The 1996 federal Health Insurance Portability and Accountability Act (HIPAA) mandated the development of federal regulations to be adopted by the U.S. Department of Health and Human Services (DHHS). The regulations were confirmed by the Secretary of DHHS in April 2001, and are effective April 14, 2003. The implementation date for small health plans is April 14, 2004.

In addition to the PRC's Fact Sheet 8a, HIPAA Basics: Medical Privacy in the Electronic Age at www.privacyrights.org/fs/fs8a-hipaa.htm, the DHHS Office of Civil Rights has published extensive information on HIPAA, available at its web site, www.hhs.gov. Click on "Questions" in the upper-right corner of the home page and follow the links to "Privacy of health information / HIPAA." Additional information can be found at the DHHS "What's New" web page, www.hhs.gov/ocr/hipaa/whatsnew.html.

A hotly debated provision of HIPAA was the creation of a national health care identification number for everyone. That is currently on hold due to strong opposition by the public and members of Congress.

Electronic health records: What are the benefits and dangers for consumers

In January 2005 the Bush Administration called for the creation of a nationwide network of electronic health records (EHR) within 10 years.

There are both benefits and very real pitfalls to such a grandiose scheme. Certainly, access to electronic records would have greatly assisted emergency health teams in the aftermath of Hurricane Katrina in August 2005. And most individuals can easily envision the benefits to hospital emergency rooms when assisting unconscious patients. But the challenges regarding security and confidentiality are profound.

To become better informed about this national initiative, visit these web sites:

Government resources:

- U.S. Dept. of Health & Human Services (DHHS) information technology page, www.hhs.gov/healthit
- The DHHS's creation of the American Health Information Community, AHIC: www.hhs.gov/healthit/ahic.html
- DHHS Secretary Leavitt's announcement of funding for development of standards for electronic health records: www.hhs.gov/news/press/2005pres/20050606.html

More recently, Microsoft announced plans for its HealthVault Web site. HealthVault is a new service for storing, managing, and accessing a patient's medical information. www.healthvault.com It operates as an online encrypted service. The service offers a voluntary opportunity for medical records to be collected by aggregating information from various sources including health-care providers, insurance companies, and compatible medical devices (such as blood pressure monitoring devices). Google intends to offer a similar service.

These types of aggregated electronic health records pose a number of concerns:

- The custodian of the records may not necessarily be a "covered entity" under the HIPAA privacy rule. HIPAA only applies to health care providers, health plans, and health care clearinghouses. Therefore, it is possible that consumers may not have any privacy rights under the HIPAA law if they utilize a service that electronically aggregates medical records.
- The Web site operator could become subject to judicial process and can be served with a subpoena for your personal medical records. This greatly facilitates the ability of both government entities and civil litigants to go on "fishing expeditions" for your medical records.

- The Web site's privacy policy can be changed at any time. This could, for example, subject consumers to targeted advertising based upon their medical conditions.

Resources for additional information

HIPAA

U.S. Department of Health and Human Services
Office of Civil Rights
200 Independence Avenue, S.W.
Washington, D.C., 20201
Phone: (866) 627-7748
Web: www.hhs.gov

Read PRC Fact Sheet 8a, "**HIPAA Basics**: Medical Privacy in the Electronic Age," www.privacyrights.org/fs/fs8a-hipaa.htm.

Contact the **U.S. Department of Labor** regarding privacy of medical information in the workplace, including your employer's health and safety files and family-leave records.

U.S. Department of Labor
200 Constitution Ave., NW
Washington, DC 20210
Phone: (866) 4USA-DOL (866-487-2365)
Web: www.dol.gov
Web link to 50 states' Labor offices:
www.dol.gov/esa/contacts/state_of.htm

Contact the **Federal Trade Commission** to learn about health information collected for:

- Employment background checks,
www.ftc.gov/bcp/online/pubs/buspubs/credempl.htm
- Applications for insurance coverage,
www.ftc.gov/bcp/online/pubs/buspubs/insurers.htm

For help with the federal **Americans with Disabilities Act**, call the nearest Technical Assistance Center.

- Phone: (800) 949-4232

- Web: www.adata.org, and for the western states, www.pacdbtac.org.

State medical boards:

- In California, for health privacy-related disputes regarding doctors, contact the Medical Board of California at (800) 633-2322. Web: www.medbd.ca.gov
- Complaints about California HMOs can be filed with the Department of Managed Health Care. Phone: (888) 466-2219. Web: www.hmohelp.ca.gov.
- To link to medical boards in the 50 states, the American Medical Association. Web: www.ama-assn.org/ama/pub/category/2645.html

Other Resources

The **Health Privacy Project** is a resource for information on medical records confidentiality. Its web site includes information on federal HIPAA regulations as well as state laws of all 50 states. Web: www.healthprivacy.org

Georgetown University's Center on Medical Records Rights and Privacy offers state-specific guides on accessing your medical records, <http://hpi.georgetown.edu/privacy/records.html>.

The **World Privacy Forum** examines the relationship between privacy, security, confidentiality and electronic health records. www.worldprivacyforum.org

HIPAA FAQ. An industry web site, HIPAAAdvisory, offers a useful FAQ. Web: www.hipaadvisory.com/action/faqs/FAQ_Main.htm.

The **Medical Privacy Coalition** is a national partnership of organizations concerned about the threat to Americans' right to protect their medical information. It is critical of HIPAA Privacy Rule. Web: www.medicalprivacycoalition.org