

HIPAA Basics: Medical Privacy in the Electronic Age

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

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

Contents:

1. [Introduction](#)
2. [HIPAA Privacy Rule - Benefits and Shortcomings](#)
3. [Who Is Covered by HIPAA? Who Is Not Covered?](#)
4. [Medical Information: What Does HIPAA Cover? What Is "Protected Health Information?" What Is "Minimum Necessary?"](#)
5. [Control of Your Medical Information: "Consent" and "Authorization"](#)
6. [More About Your Right to Access Your Medical Records](#)
7. [HIPAA and Your Employer](#)
8. [HIPAA and the Government](#)
9. [HIPAA and Your Credit Report](#)
10. [HIPAA and Your Daily Routine](#)
11. [Complaints and Penalties](#)
12. [The HIPAA Security Rule](#)
13. [Electronic Health Records \(EHR\)](#)
14. [The 2009 Stimulus Bill, Electronic Health Records, and Privacy](#)
15. [Tips for Safeguarding Your Medical Information](#)
16. [References and Resources](#)

1. Introduction

Today, you have more reason than ever to care about the privacy of your medical information. Intimate details you revealed in confidence to your doctor were once stored in locked file cabinets and on dusty shelves in the medical records department.

Now, sensitive information about your physical and mental health will almost certainly end up in data files. Your records may be seen by hundreds of strangers who work in health care, the insurance industry, and a host of businesses associated with medical organizations. What's worse, your private medical information is now a valuable commodity for marketers who want to sell you something.

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996 to set a national standard for electronic transfers of health data. At the same time, Congress saw the need to address growing public concern about privacy and security of personal health data. The task of writing rules on privacy eventually fell to the U.S. Department of Health and Human Services (HHS). After several modifications, DHHS issued the HIPAA Privacy Rule.

The Privacy Rule was effective on April 14, 2003, for most health care providers, health plans, and health care clearinghouses. Small plans have until April 14, 2004, to comply.

If you expect HIPAA to restore your confidence that sensitive medical data is a matter between you and your doctor, you will be disappointed. HIPAA sets the standard for privacy in the electronic age where health industry, government, and public interests often prevail over the patient's desire for confidentiality.

This guide explains the complex provisions of HIPAA's Privacy Rule. It covers HIPAA's high points and low points regarding your health privacy. For more information on HIPAA and additional rules that are not explained here, go to the [References](#) section at the end of this guide.

2. HIPAA Privacy Rule - Benefits and Shortcomings

What does HIPAA do? Is it good or bad?

The final version of the Privacy Rule includes both good and bad news for consumers. You may be surprised to see the *new* privacy "rights" in HIPAA were ones you always thought you had. The following provisions are HIPAA's "high points."

1. **HIPAA sets a national standard** for accessing and handling medical information. Before HIPAA, your right to privacy of health information varied depending on what state you live in. Now, health care providers, health plans and other health care services that operate in all states have to abide by the minimum standards set by HIPAA.

Your state is free to adopt laws that give you *more* privacy, but it cannot take away the basic rights given by HIPAA. It is likely that your state has existing laws that in some way govern the privacy of medical records. Some states may pass new laws to incorporate or strengthen HIPAA. To find out what the laws are in your state, visit the web site of the Health Privacy Project of Georgetown University, www.healthprivacy.org, and select the section for State Law. Determining whether a state has a law that remains in force after the HIPAA Rule can be a challenging task, even for experienced lawyers.

2. **Access to your own medical records**, prior to HIPAA, was not guaranteed by federal law. Only about half the states had laws requiring patients to be able to see and copy their own medical records. Now HIPAA gives everyone the right to see, copy, and request to amend their own medical records. You can be charged for copies of your records, but HIPAA sets limits on the fees. For more on access to your medical records, see [Part 6](#) of this guide.
3. **Notice of privacy practices** about how your medical information is used and disclosed must now be given to you. You should get a notice the first time you visit your doctor after the HIPAA Privacy Rule takes effect. The notice should also be available in the health care facility. It must tell you how to exercise your rights under the Rule. And the notice must explain how to file a complaint with your health care provider and with the HHS Office of Civil Rights.
4. **An accounting** of disclosures of your health information is also required by HIPAA. You can find out who has accessed your health records for the prior six years, although there are several exceptions to the accounting requirement. For example, accounting is not required when records are disclosed to the many individuals who

see your records for treatment, payment, and health care operations (TPO). Those involved in TPO do not need to be listed in the disclosure log.

5. **You can file a complaint** with your health care provider and/or with the HHS if you believe a health care provider or health plan has violated your privacy. Go to [Part 10](#) and the [References](#) section at the end of this guide for more information on filing complaints.
6. **Special requests for confidential communications should be granted, if reasonable.** You might prefer that telephone calls about your treatment be made to your home rather than your office. Or you might want notices like appointment reminders sent to a post office box instead of your home address.
7. **Staff training, the appointment of a privacy officer** , and establishment of formal **safeguards** are some of the administrative requirements organizations must comply with under the HIPAA Privacy Rule. These new requirements impose a focus on privacy that may have taken a back seat in the hectic, business-like atmosphere that often characterizes modern-day health care.
8. **You** have a choice when it comes to having your name included in a hospital directory. You can also choose to have your medical information discussed with designated immediate family members, close friends, or relatives.
9. **Penalties**, both civil and criminal, are authorized by the HIPAA Privacy Rule if the government brings a lawsuit for violations. The penalties, if imposed, could provide an incentive for compliance with the Privacy Rule. (See [Part 10](#).)

What are HIPAA's shortcomings?

Like it or not, you are not the only one with an interest in control of personal health information. The balancing act between your interests and those of other stakeholders is often tipped on the side of government, the medical profession, related businesses, and public interests. Consumer and patient advocates are critical of HIPAA for its numerous weaknesses.

Here are some of the ways that patients' rights to privacy come up short:

1. Your consent to the use of your medical information is *not* required if it is used or disclosed for treatment, payment, or health care operations (TPO). In many situations such as emergencies, this makes perfect sense. You don't expect the ambulance driver to get your permission to call the hospital emergency room when you are having a heart attack. On the other hand, since your consent is not required for payment, your health care provider could submit a claim to your insurance company - even for a procedure you wanted to keep private and intended to pay for yourself. In addition, treatment, payment, and health care operations have broad definitions that encompass many activities that most people are not familiar with.
2. **Your past medical information** may become available, even if you thought the information was long buried and would remain private. An event, treatment, or procedure from your distant past can be disclosed the same as information about current conditions. Of some comfort, old information is given the same protections under HIPAA as current information. In addition, HIPAA's "minimum necessary" rules

applies to old as well as new records. This means that the amount of information disclosed should be limited to what is necessary to accomplish the purpose.

3. **Your private health information can be used for marketing** and may be disclosed without your authorization to pharmaceutical companies or businesses looking to recall, repair or replace a product or medication. (For more on the marketing of your medical information see [Part 5](#) below.)
4. **You have no right to sue under HIPAA** for violations of your privacy. In other words, you do not have a "private right of action." Only the HHS or the U.S. Department of Justice has the authority to file an action for violations of the Privacy Rule. All you can do is complain to the one who violates your privacy or to the HHS. However, you may be able to sue under state law using the HIPAA Privacy Rule to establish the appropriate standard of care.
5. **Business associates** of a covered entity can receive protected health information (PHI) without a patient's knowledge or consent. Before entering into an agreement with a business associate, a covered entity must receive assurance that information will be handled appropriately, After that, handling of sensitive data by business associates is left only to an honor system. Even when the limitations of the Privacy Rule are applied, many people can still see your medical records when carrying out the business of the plan or provider. Business associates may include billing services, lawyers, accountants, data processors, software vendors, and more. Your doctor may, for example, disclose your health information to a business associate that processes medical bills. A written contract for this arrangement is required, but the doctor doesn't have to check to see that your information is being handled correctly. If there is a violation, the business associate is supposed to report it.
6. **Law enforcement** access to protected health information under HIPAA is a significant concern of privacy and civil liberties advocates. Some disclosures may be made to law enforcement without a warrant or court order.

3. Covered Entities

Is everyone involved in my health care covered by HIPAA?

No. The HIPAA Privacy Rule pertains to three categories of "covered entities" - health care providers, health plans, and health care clearinghouses.

1. Health care providers are covered if they transmit health information *electronically*. Even a doctor in a small practice who keeps only paper records will almost certainly use a billing service that transmits information electronically. In short, it is nearly impossible to provide health care today without using electronic means in some way.

As long as information is transmitted electronically, "health care provider" includes your doctors, hospitals, staff involved in your treatment, laboratories, pharmacists, dentists, and many others that provide medical, dental, and mental health care or treatment. In short, a provider is almost anyone in the business of providing health care who is licensed or regulated by the states.

2. Health plan means almost anyone that pays for the cost of medical care. This includes: health insurance companies, HMOs (health maintenance organizations),

group health plans sponsored by your employer, Medicare and Medicaid, and virtually any other company or arrangement that pays for your health care.

3. Health care clearinghouses can be any number of organizations that work as a go-between for health care providers and health plans. An example of this would be a billing service that takes information from a doctor and puts it into a standard coded format. Patients rarely deal directly with clearinghouses.

An organization may also be what is called a hybrid entity. A hybrid entity provides health care as *only part* of its business. A large corporation that has a self-insured health plan for its employees is one example of a hybrid entity. Only the portion of the company that processes claims and makes payments to health care providers is subject to the HIPAA Privacy Rule.

Who is *not* covered by the HIPAA Privacy Rule?

Your medical information may be available to many who are *not* covered by HIPAA. Here are some examples of who is *not* covered.

- Life insurance companies.
- Workers Compensation.
- Agencies that deliver Social Security and welfare benefits.
- Automobile insurance plans that include health benefits.
- Internet self-help sites.
- Those who collect health data you give voluntarily for surveys or research projects.
- Those who conduct screenings at pharmacies, shopping centers, hometown fairs, or other public places for blood pressure, cholesterol, spinal alignment, and so on.
- Researchers who obtain health data directly from health care providers.
- Law enforcement agencies.

Even though these institutions are not covered by HIPAA, they may get information from a covered entity.

Is the Medical Information Bureau (MIB) a covered entity? What about IntelliScript and MedPoint?

No. The MIB is a member organization made up of insurance companies. Because the MIB is neither a health care provider, health care plan, nor health care clearinghouse, it is not a covered entity. Most of MIB's members underwrite life and disability insurance, functions that are not covered by HIPAA.

MIB's activities falls under another federal law, the Fair Credit Reporting Act (FCRA) because the company gathers information and issues reports about individuals to insurance companies. Two other companies that fall under the FCRA are Milliman, owner of the IntelliScript database, and Ingenix, Inc. owner of the MedPoint database. The IntelliScript and MedPoint databases gather information about a consumer's prescription drug history and issue reports to insurance companies.

For more on MIB, see www.mib.com and Privacy Rights Clearinghouse Fact Sheet 8, "*How Private Is My Medical Information?*" www.privacyrights.org/fs/fs8-med.htm.

For more on MedPoint, see www.ingenix.com/ContactUs/

For more on IntelliScript see www.rxhistories.com/how_it_works.html

4. Medical Information - What Does HIPAA Cover?

What kind of information is covered by the HIPAA Privacy Rule?

HIPAA covers any information about your past, present or future mental or physical health including information about payment for your care. To be covered by HIPAA, information has to be kept by a covered entity - a health care provider, health care plan, or health care clearinghouse. This, combined with some fact that identifies you (your name, address, telephone number, Social Security number) is called "protected health information" or PHI. PHI can be oral, handwritten, or entered into a computer. This means a conversation between a doctor and nurse about your condition has the same general protections as information written on your records.

Are my child's (K-12) records of visits to the school nurse covered by HIPAA?

No. Health records kept by schools are classified as "education records" covered by the Family Educational Rights and Privacy Act (FERPA). For more on FERPA and privacy of your child's education records, visit the US Department of Education web site, www.ed.gov/offices/OM/fpco/ferpa/index.html.

Are there any limits on what can be disclosed from my medical file?

The Privacy Rule incorporates what it calls a "minimum necessary" standard when it comes to how much information should be disclosed. Doctors, hospitals, and others covered by the HIPAA Privacy Rule are required to limit the amount of information disclosed to others to the *minimum necessary* to accomplish the intended purpose.

What amounts to the minimum is left up to the health care provider, not you. And, the minimum necessary rule does not apply to information disclosed in connection with treatment. It also doesn't apply if you authorize the disclosure of your health information.

5. Control of Your Medical Information: "Consent" and "Authorization"

Your ability to control how your medical information is used falls generally into four different situations - along a continuum of *no control* to *some control* :

- There are situations where you have *no* right to consent.
- In some situations your authorization *is not needed*.
- In certain cases your authorization *is* needed.
- You have an opportunity to consent or object in a few situations.

The HIPAA Privacy Rule makes a distinction between your "consent" and your "authorization." An authorization must be given on a separate document that sets out details of the disclosure.

Consent, when required, is much less formal (discussed further below.) To see how HHS explains the difference between consent and authorization, visit the Question and Answer Section of the Agency's web site. Select the category "Privacy of Health Information/HIPAA" and the subcategory of "Authorizations," http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php

When can information be used without my consent?

Consent for use of your information is not the same as consent for treatment. The HIPAA Privacy Rule does not change the general requirement that a health care provider needs your consent before treating you.

A covered entity is allowed to seek your consent, and some state laws require patient consent for treatment, payment, and other disclosures. A covered entity is required to make a good faith effort to obtain your acknowledgment that you received a notice of privacy practices, but this is not the same as obtaining consent.

Your consent is not required when your medical information is used for treatment, payment, or for health care operations (TPO). But it goes much further than that. Your consent is not necessary when your information is used by a business associate of your health care provider or plan.

Services provided by a business associate can include: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. These business relationships are established with a written contract. Your personal medical information can be used to carry on the business association, but you are not a party to the arrangement.

Does HIPAA allow a provider to contract with a foreign business associate ?

HIPAA makes no distinction between a U.S. business associate and one based in a foreign country. Of late, outsourcing services that involve the transfer of personal data offshore have been the subject of many press reports. Legislation has been introduced in Congress and some state legislatures to at least give consumers notice when medical data is sent offshore. For many Americans, outsourcing is most troubling when the services provided by a foreign company entail the use of highly sensitive medical and financial information. However, to date, there are no legal restrictions on outsourcing medical-related services.

What does "health care operations" mean?

Health care operations are not the same as business associate arrangements. Use of your medical information for purposes of carrying out operations does *not* require a written contract. Here are just some of the things that fall under the broad heading of operations:

- Reviewing the competence of health care professionals.
- Training programs.
- Activities related to health care contracts.
- Business planning and development.
- Resolution of internal grievances.
- Sale, transfer, merger, or consolidation of the health care provider or plan.
- Medical services review, legal services, auditing, including fraud detection.

- Fundraising.

Will I ever know how many people have seen my medical information?

HIPAA requires safeguards to limit the number of people who have access to personal information. Given the number of people who may have access to your information just to run the operations and business of the health care provider or plan, there is no realistic way to count the number of people who may come across your records. If you are hospitalized, for example, hundreds of hospital employees may see your health information.

When you add to this the number of instances listed below in which your medical information can be disclosed without your authorization, the numbers can be staggering. For an idea of how extensive routine disclosures can be, read "Health Privacy: The Way We Live Now" by Robert Gellman, reprinted on the Privacy Rights Clearinghouse web site, www.privacyrights.org/ar/gellman-med.htm.

Can my PHI be disclosed without my authorization?

The HIPAA Privacy Rule carves out many exceptions to your ability to authorize release of your "protected health information," including *details that identify you*. As discussed earlier, you don't have the right to consent or object when your information is used for treatment, payment, or operations, including disclosures to business associates of your health care provider or plan. Each of these exceptions places conditions on the covered entity who makes the decision to disclose. But, you are out of the loop.

The flow of your medical information is beyond your control when the disclosure is made by a covered entity to or in connection with:

- Any disclosure required by federal, state, or local regulation, regardless of the scope of the disclosure or the purpose of the disclosure.
- Public health authorities.
- A person subject to the jurisdiction of the federal Food and Drug Administration.
- A person who may have been exposed to a communicable disease.
- An employer to (1) conduct workplace medical surveillance or (2) to evaluate whether you have a work-related illness or injury.
- Victims of abuse, neglect or domestic violence.
- A health oversight agency for audits and investigations.
- Court or administrative proceedings in response to a court order, subpoena, or discovery request.
- A collection agency for unpaid medical bills.
- Coroners and medical examiners.
- Funeral directors.
- Organ procurement organizations.
- A medical researcher with institutional review board approval.
- A threat to public safety or public health.
- U.S. and foreign military commanders.
- U.S. Department of Veterans Affairs to determine eligibility for benefits.
- Federal government national security and intelligence officials.
- U.S. Department of State to verify health fitness of employees and their families for foreign duty.
- Correctional institutions involved in health care of inmates.
- Workers compensation uses authorized by state law.

Further .

- Law enforcement access is authorized in a number of ways under HIPAA. In some cases information may be disclosed without a warrant or court order.

Obviously, many of the disclosures listed above are made for the public good. Some disclosures are required by law. Who could argue, for example, with the need to alert public health officials to an outbreak of a deadly disease. And, there is without a doubt a strong public interest in mandatory reporting of suspected child abuse.

Each one of the disclosures listed above that can be made *without the authorization* of the subject carries with it a set of conditions. For a complete list of those conditions, you may want to look at §164.512 the Privacy Rule itself, www.hhs.gov/ocr/regtext.html. If you still have a question, you can visit the HHS web site and submit a question, www.hhs.gov/ocr/hipaa/finalreg.html. But, be aware, there are many questions that remain unanswered about HIPAA.

Is my authorization *ever* required before my information can be disclosed ?

HIPAA requires your specific authorization unless disclosure is not otherwise allowed. Special authorization requirements apply (1) when the disclosure involves psychotherapy notes and (2) when the disclosure is made for marketing.

The Privacy Rule explains the procedure that must be followed to get your authorization. It states that you should not be denied treatment because you decide not to sign the authorization.

- **Psychotherapy notes** should not be disclosed to others without your authorization. Again, there are built-in exceptions if the notes are used for such purposes as training staff or to defend the doctor or health plan in court.
- **Marketing**, or when someone tries to sell you something based on your health information, is allowed if you give your authorization. But, there's often a fine line between marketing that requires your consent and marketing that does not.

Following are some examples from the HHS web site of what *is* and *is not* considered marketing under the Privacy Rule:

Examples of marketing communications *requiring* prior authorization:

1. A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a baseline EKG for \$39, when the communication is not for the purpose of providing treatment advice.
2. A communication from a health insurer promoting a home and casualty insurance product offered by the same company.

It is *not* marketing and no authorization from you is required when :

1. A hospital uses its patient list to announce the arrival of a new specialty group (for example, orthopedic) or the acquisition of new equipment (like a magnetic resonance image machine) through a general mailing or publication.
2. A health plan sends a mailing to subscribers approaching Medicare-eligible age with materials describing its Medicare supplemental plan and an application form.

The term "marketing" is one area that is likely to be debated by state legislators given states' authority to expand HIPAA privacy protections. California lawmakers have already proposed to strengthen the HIPAA marketing provisions during the 2003 legislative session, www.leginfo.ca.gov (Assembly Bill 262).

Can I be denied treatment or coverage if I don't give my authorization?

No. Treatment or health care coverage cannot be denied because you don't sign an authorization. Again, there are exceptions. If the authorization is for research-related treatment, you may not be allowed to participate in the research program without giving authorization to disclose your information. If authorization is requested from a health plan *prior* to the time you enroll and you refuse to give your authorization, you may not be allowed to enroll.

Can I revoke my authorization?

Yes, if you do so in writing and *before* any action is taken based on your authorization.

Does a hospital need my authorization to include me in a directory?

We explained above about two opportunities to authorize release of your personal data - psychotherapy notes and certain marketing situations. Another situation is created under HIPAA for "directory" information.

That situation typically arises when you are admitted to the hospital. Hospitals routinely maintain directories, and inquiries are often made about a patient from a member of the clergy, the news media, family, and friends. If you are not in the directory, the hospital will not be able to tell visitors you are there, route phone calls, deliver flowers, and so on.

Situations in which individuals are likely to want to limit the disclosure of directory information include: victims of domestic violence or stalking who need to safeguard their location, celebrities and other public officials who want their hospital stay kept private, and individuals who for whatever reason want to limit others' knowledge of their health condition. Under the HIPAA Privacy Rule, you must be given an opportunity to either agree or disagree to the disclosure of your directory information.

When can I agree or disagree to having "directory" information about me disclosed?

You should be given this choice as part of the admission procedure. The directory could include information about your location within the facility, your religious affiliation (disclosed to members of the clergy only), and your condition. An agreement to be included in a hospital directory may be made orally or in writing. You can restrict the kinds of information to be disclosed and to whom it is disclosed. In case of an emergency or another situation where you are not able to give your consent, your health care provider may use his or her

professional judgment. In that case, you should be consulted later when you are able to make an informed choice.

For more on hospital directories, see Myth #3 on the Health Privacy Project web site at www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm?doc_id=173435

Can I give consent or authorization for someone else?

Yes, in some circumstances. The HIPAA Privacy Rule includes information on when you can act for another person or when someone can act for you. This might include times when you have a power of attorney, when you are the parent of a minor child or mentally retarded adult, or when you or someone else is acting in an emergency. For more on this, see the section on [References](#) below and go to the HIPAA web site for "Personal Reps/Parents and Minors."

What documents will I have to sign?

The Privacy Rule includes only one situation where the consumer *has* to sign a document. As discussed above, a patient must sign an authorization form before health information can be disclosed for marketing or when psychotherapy notes are involved.

It is also standard for a consumer to be asked to sign a form acknowledging that he or she has received a copy of the provider's privacy policy. However, the regulation says only that the covered entity must make a "good faith" effort to obtain a signed acknowledgement form.

A signed acknowledgement means only that the consumer/patient was given a copy of a privacy notice. It does not mean (and should never state) that the consumer agrees with the policy. If the patient does not sign the acknowledgement, the covered entity is supposed to document the "good faith" effort. We have learned of instances where a covered entity has refused to provide services if the patient refuses to sign an acknowledgement. The Privacy Rule does not give the healthcare institution the right to deny service to a patient who refuses to sign a document acknowledging that they received a copy of the notice.

6. More About Your Right to Access Your Medical Records

Your ability to see your own medical records is probably the single most important right you have under HIPAA. Before HIPAA, your right to see or copy your medical records often depended on your state laws. Now, HIPAA sets the national standard, or *floor*, meaning that states can give you greater rights to access your medical information, but state laws cannot take away the fundamental access rights you have under HIPAA.

Does HIPAA allow me to get my original records?

No. HIPAA only gives you the right to get copies of your records. Or, if you choose, you can ask to see your medical records or ask for a summary of your medical file.

Do I have to submit a written request for my medical records?

HIPAA does not require a written request. However, if your provider requires a written request, you must be given notice of this. Some providers may have a form specifically for

this purpose. Or, the provider's privacy policy should tell you how to request your medical records.

Even if your doctor does not require a written request, it is always a good idea to put your request in writing. That way, you have a record of important details such as when you filed your request and the record you requested. For a sample letter to request a copy of your medical records, see www.privacyrights.org/Letters/medical2.htm.

When will I get my records?

Usually, you should get your copies within 30 days of the request. Under HIPAA, if the process takes more than 30 days, you must be given a reason. Your state law may give you the right to receive your records more quickly. In California, for example, you should be able to see your medical records within 5 days and get a copy within 15 days. For more on your rights to access under state laws, see <http://hpi.georgetown.edu/privacy/records.html>.

Do I have to pay for copies of my medical records?

Probably, yes. HIPAA says you can be charged a reasonable, cost-based fee.† This means you can be charged for supplies and staff time for copying your records. You can also be charged for mailing records, if mailing is what you request. But, you should not be charged for time spent searching for your records. Nor, should a provider have a policy of charging all patients a flat fee.

Do I have to pay for a summary of my medical file?

Yes, but you must agree to the fee in advance.

Can I be denied access to my medical records?

Yes, in a few circumstances. For example, you cannot access psychotherapy notes or information compiled for lawsuits. Your request can also be denied if the provider decides the information you want could reasonably endanger your life, your physical safety or that of another person. A written denial letter is usually required. In some cases, you can appeal a denial. If so, you should be given instructions on how to appeal in the written denial.

Does HIPAA say medical records must be kept for a certain time?

HIPAA does not include a record retention period. It does, however, allow you to request an accounting or report of who has accessed your records. This covers the six years prior to the date you request the accounting.

How do I correct inaccurate information in my medical records?

You can ask for a correction of inaccurate information. You should make your request in writing. You should receive a written answer within 60 days. If your correction request is denied, you can note your disagreement in your file.

My physician is no longer in practice. How do I find my records?

The American Health Information Management Association, www.ahima.org, offers the following advice on how to locate records when your physician is no longer in practice:

Even if your physician moved, retired, or died, his or her estate has an obligation to retain your records, including immunization records, for a period defined by federal and state law. Often this retention period is 10 years following your last visit (or until a child/patient is 21). You may be able to locate your records by contacting:

- Your physician's partners
- The health information manager at a nearby hospital where the physician practiced
- The local medical society
- The state medical association
- The state department of health
www.myphr.com/faqs/index.asp#5

Since I am caring for my elderly parents, may I request their medical records?

Generally, permission to access another person's medical records must come from the patient. The patient may designate a friend or relative to receive information related to care and treatment. Permission should be given in writing and filed with the care provider or facility. If the patient is incapacitated, you or another person may be appointed legal guardian by a court. Then, the legal guardian decides who has access to the patient's medical records.

Is it possible to access medical records of a person who is deceased?

HIPAA speaks of two instances that allow access to a deceased's medical files. One, the personal representative designated by a will or appointed by a court to settle the deceased's affairs may gain access to medical files. Second, a relative may receive medical information about the deceased if the information has a bearing on the relative's health.

Do I have the right to see my child's medical records?

Generally, yes. However, there are some exceptions:

- When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law.
- When the minor obtains care at the direction of a court or a person appointed by the court.
- When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

Additional information about a minor child's health records can be found on the HHS web site, www.hhs.gov/ocr. Under "Health Information Privacy," click the link to "Frequently Asked Questions about Privacy of Health Information," and then enter the words "minor" or "child" into the search block.

The Guttmacher Institute has a guide to state laws, "Minors and the Right to Consent to Health Care" available at www.guttmacher.org/pubs/tgr/03/4/gr030404.pdf (2000).

7. Your Health Records and Your Employer

For many people, the ultimate worry is that an employer's access to information about health and treatment or even the possibility of future illness can affect employment. The way and extent to which the HIPAA Privacy Rule covers your health information in the workplace depends on the type of health coverage you have. The majority of people in the workforce who have health benefits associated with employment fall into one of two categories:

- Group health plans are covered by the HIPAA Privacy Rule as long as the plan has 50 or more participants. If you are a member of a group health plan, your employer pays a premium to the health plan organization to cover your health care costs. In return for the premium paid, the health care plan assumes the risk of paying for health care expenses covered by the plan. The HIPAA Privacy Rule applies to the plan itself, but not your employer.
- **Self-insured plans** are health plans often offered by large employers as an employee benefit. Under self-insured health plans, the employer itself assumes the risk of health care costs and has the responsibility for paying health care claims out of the company's operating funds. Claims may be processed by company personnel or contracted out to other companies that process and maintain the records.

My employer sponsors a group health plan? Can my boss see my medical claims?

HIPAA says that the group health plan can tell your employer whether you are enrolled in the plan or not. Your employer can also get from the group plan what is called "summary" information to use to obtain premium bids or changes in coverage. If the health information your employer receives goes beyond the basic summary, then HIPAA requires the employer to establish procedures much like that of a covered entity. HIPAA attempts to limit the use of medical information for employment purposes.

My employer is self-insured. Does HIPAA guarantee my privacy?

Under the HIPAA Privacy Rule, an employer that is also the insurer of health benefits is in a category called a "hybrid" entity. That means the portion of the company's operations that deal with processing health claims is a covered entity. Like any other covered entity, a "hybrid" function must (1) give notice of written privacy procedures, (2) place restrictions on the use of health information, and (3) appoint a privacy officer and train staff.

Can my self-insured employer see my health claims?

If you are the least bit concerned about the privacy of your medical information, the close relationship between your boss and the person who processes your health claims can send a chill down your spine.

It's Helen in personnel who's looking at all the forms, and knows whether you're seeing a psychiatrist, you just had your tubes tied, or you've just been diagnosed with cancer," quoting the chairman of the University of Massachusetts Medical School Psychiatry Department in *National Journal*, "Open Secrets," (Oct 9, 1999) at p.2880.

HIPAA requires that "hybrid" entities such as self-insured employers erect "firewalls" between the portion of the company that handles the health claims and the portion that does

not. However, the effectiveness of this procedure remains to be seen. The threat to privacy posed by self-insured employers was the subject of a report prepared by Congressional Representative Henry Waxman in April, 2002, "Medical Privacy Policies of Large Corporations Have Major Deficiencies,"

www.house.gov/reform/min/pdfs/pdf_inves/pdf_privacy_rep.pdf.

My employer has an on-site health clinic. Is that covered by HIPAA?

An on-site health clinic at your place of employment may be another example of what the HIPAA Privacy Rule calls a "hybrid" entity. This depends on whether the health clinic transmits information electronically and engages in standard transactions under HIPAA's electronic data interchange rule, for example, if the clinic bills an employee's health plan. If so, the records maintained by the health clinic are subject to the same protections that apply to other covered entities.

Are all records related to my employment and my health subject to HIPAA?

No. Records that relate to other employee benefits such as life insurance, disability, workers compensation, or long-term care insurance are not covered by HIPAA. Nor are records that relate to your employer's compliance with laws that govern safety and health risks in the workplace.

I work in a hospital. Is my employment file covered by HIPAA?

No. The Privacy Rule applies only to records maintained for treatment of patients. Records in your employment file are not covered.

8. Your Health Records and the Government

There are many situations when the government has the right or the legal obligation to see your medical records. State agencies must keep records of births and deaths as well as registries of people who have been diagnosed with serious illnesses such as cancer or HIV. Typically, disclosures to the government do not require your authorization. (See [Section 4](#) for some examples of when government officials can see your medical records.)

Many government-sponsored health programs such as those covering the military, veterans, and government employees are covered by the Privacy Rule. When personally identifiable health information is collected by the government, the federal Privacy Act also applies.

HHS, a federal government agency, may have access to your health records in connection with an investigation. The agency's Office of Civil Rights (OCR) reviews complaints about privacy violations. You might complain to the OCR, for example, that your HMO refused to give you a copy of your medical records. Then, OCR could request a copy of your records from your HMO as part of its investigation.

Does HIPAA create a government database of medical information?

Following is quoted from the HHS web site on the subject of medical databases:

Does the HIPAA Privacy Rule create a government database with all individuals' personal health information? Answer No. The Privacy Rule does not create such a government

database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation.

9. Your Health Information and Your Credit Report

Can my information be disclosed to a collection agency?

Yes. When you put on that faded cotton gown and sit on the examining table, you are the patient. But, your role could change to many other things, including that of debtor. You visit your doctor and pay for health insurance premiums so that you are assured of care in an emergency or in case of an illness. But, your relationship is also a business arrangement.

You are obligated to pay for any costs not covered by your health insurance. *Remember* : Your consent is not required to disclose information from your medical files if it is made in connection with payment.

An unpaid bill, like any other debt claimed to be owed, may be reported to a collection agency. What's more, an unpaid medical bill can appear as a negative entry on your credit report. Information that can be disclosed to a collection agency about you includes:

- Your name and address
- Date of birth
- Social Security number
- Payment history
- Account number
- Name and address of the health care provider or health plan that says you owe the money.

A recent study by the Federal Reserve found that over half of all collections noted on credit reports were for unpaid medical bills, www.federalreserve.gov/pubs/bulletin/2003/0203lead.pdf.

Can I dispute a medical bill?

Unfortunately, the federal law that enables consumers to dispute billing errors does not apply to medical bills. The Fair Credit Billing Act only applies to credit cards accounts and revolving charge accounts. But that does not mean that you cannot dispute billing errors.

The medical billing and insurance claims processes can be complicated and confusing. Be sure to stay on top of your medical bills and dispute matters *in writing* with both the health provider and insurance company when you think errors have been made. Try to get the matter resolved *before* the debt is reported to a collection agency and/or to the credit reporting agencies (Experian, Equifax, TransUnion).

If a medical debt is reported to a collection agency, you have rights given by credit and collection laws. Federal laws are the Fair Credit Reporting Act and the Fair Debt Collection Practices Act. State laws might also apply.

For more information about your rights under these consumer protection laws, visit the Federal Trade Commission's web site at www.ftc.gov. You can also learn more about credit reports and your right to dispute negative information by reading the Privacy Rights

10. HIPAA and Your Daily Routine

HIPAA touches nearly every aspect of modern medicine. Privacy in the hotly debated issues of medical research and genetic testing are beyond the scope of this guide. For more information on these topics, see the HHS web site and the [References](#) Section at the end of this guide.

But HIPAA also touches on privacy in small ways like routine office visits, prescription refills, and messages left on voice mail systems. This is a partial list of day-to-day situations that may or may not be changed by HIPAA:

- You can make a special request to be called for appointment reminders or to discuss your treatment at a certain telephone number.
- Your health care provider should be careful to keep information left on patients' voice mail systems to a minimum.
- Medical records can be faxed from one doctor to another.
- Someone else can pick up your prescription with your permission.
- Your doctor can prescribe medication without a face-to-face visit.
- The pharmacists can talk to you over the counter about your medication, but must take care that others near you do not hear the conversation.
- Medical files can be left outside the examining room, but should be turned facing the wall.

Will HIPAA stop gossip?

Rumors and gossip about medical conditions or treatment are a concern to many people. This is particularly true in small communities where neighbors, friends, and former in-laws might work at the only hospital in town. Under HIPAA, access to sensitive medical information *should* be limited to those who have a need to know. However, no system can ever stop gossip. If you find that any of your sensitive medical information is disclosed through the grapevine, you should not hesitate to report it to the health care service and file a complaint with the HHS.

Health care providers must pay attention to accidental disclosures through routine conversation. A doctor, nurse, or technician may violate the HIPAA Rule simply by saying to a third party that they saw a particular individual at the clinic last week. That statement discloses that the individual is a patient who sought care, and both of those facts are "protected health information" (PHI) under HIPAA. The disclosure might be particularly sensitive if the physician is a psychiatrist, but the same policy applies to family practitioners, pharmacists, and dental hygienists too.

11. Complaints and Penalties for Violations

What can I do if someone violates the HIPAA Privacy Rule?

You don't have the right to sue under HIPAA. The most you can do is file a complaint. The privacy notice you receive from your health care provider or plan is required to tell you how to file a complaint within the organization. The notice should also tell you how to contact the

HHS Office of Civil Rights. This is the government office charged with enforcing the Privacy Rule.

You must file your complaint within 180 days of the violation, but HHS can extend that time. HIPAA says you cannot be denied treatment because you file a complaint.

Even though the HIPAAA Privacy Rule does not give you the right to sue, other federal or state laws or regulations might give you the right to bring an action in court for violations of your privacy. If you feel your rights have been violated, you may want to discuss the situation with an attorney.

What happens after I complain?

The HHS may decide to investigate and/or try to resolve the issue informally. A person or organization that is obliged to follow the Privacy Rule may face a civil fine of up to \$25,000. In extreme cases, the U.S. Department of Justices (DOJ) may be called in to conduct a criminal investigation. If the DOJ becomes involved, violators could face a jail term of up to 10 years and a fine of up to \$250,000.

12. The HIPAA Security Rule

Privacy and data security go hand-in-hand. So far, this guide has looked at the HIPAA Privacy Rule, explaining what you *can* and *cannot* do to protect your sensitive medical files. A new regulation, also published by the Department of Health and Human Services, describes what "covered entities" *must* do to make sure your medical files are secure. The Security Rule took effect April 20, 2005, for larger entities, with a one year delay for health plans having annual receipts of \$5 million or less.

Do I have a role in the HIPAA Security Rule?

Patients receive notice about privacy practices, but data security operates behind the scenes, out of your hands. Still the Security Rule is important to patients because, like the Privacy Rule, it creates a national standard. This means that all health care providers, health plans, and health care clearinghouses that transmit information electronically must adopt a data security plan.

Does the Security Rule protect all my health records?

Only health information maintained or transmitted in electronic format is covered by the Security Rule. Paper records stored in filing cabinets are not subject to the security standards imposed by the HHS.

What does the Security Rule require of covered entities?

The Security Rule, according to the HHS, was designed to be flexible, establishing a security framework for small practices as well as large institutions. All covered entities must have a written security plan. The HHS identifies three components as necessary for the security plan. Those are:

- Administrative safeguards
- Physical safeguards

- Technical safeguards.

Each of the three major categories has a number of subcategories. Some things must be included in the security plan while other factors are "addressable," that is items that may be considered and adopted if suitable to the covered entity's size and organization.

Will I be notified about a security breach?

The Security Rule requires covered entities to adopt "incident" reporting procedures. However, it seems that this relates only to internal reporting. According to the HHS, "This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations." Thus, while the HIPAA Security Rule does not require you be notified of a breach, other laws such as California's security breach law may require notice. (CA Civil Code §1798.29)

For more on California's security breach law, see www.privacyprotection.ca.gov . Click on "Privacy Laws." For information on security breach laws in other states, visit Consumers Union's Financial Privacy Now, www.financialprivacynow.org .

For the complete text of the HIPAA Security Rule, see www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

Where can covered entities find help with understanding the Security Rule?

The National Institute of Standards and Technology (NIST) published a guide to implementing HIPAA's Security Rule in October 2008. Although NIST's guide was prepared for use by federal government entities that are subject to HIPAA, the publication also provides voluntary guidelines for use by state, local, and private entities.

NIST's Guide 800-66 is available at: <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

In addition, the Web site for the HHS Office of Civil Rights offers an abundance of educational materials for help in understanding and complying with all phases of HIPAA. www.hhs.gov/ocr/hipaa/

13. Electronic Health Records

Is my health information stored in electronic format?

Almost certainly some - or major portions of your health information - is kept in electronic format. In fact, to be covered by HIPAA at all means that protected health information is transmitted electronically, usually between a healthcare provider and a health benefit plan.

Even small medical practices are moving away from paper records. If your provider is a Health Maintenance Organization (HMO) or you have had a hospital stay, your medical information is likely to be accessed through computers accessible to various departments throughout the facility. In addition, some employers have established an internal electronic network of health data.

Is there a national database of medical records?

Not yet. But, that is the plan. In 2004 President Bush issued an Executive Order that requires the Department of Health and Human Services (HHS) to study and develop a national health information network (NHIN). With a ten-year deadline, the task of overseeing the system has been left to a newly created HHS Office, The Office of the National Coordinator for Health Information Technology, www.hhs.gov/healthit/measuring.html.

In addition to HHS efforts, a number of bills have been introduced in Congress to speed the development of and fund a national system of electronic health records.

While the NHIN is not likely to be a reality for some time, many state governments have appointed boards and task forces to study the issue. The first step will be a regional network, combining electronic health records from a number of unrelated sources. The next step will be to combine the regional networks to create a statewide network. Ultimately, the state systems will feed into the national network so that health records are available nationwide—even worldwide. See, for example, the CalRHIO project, www.calrhio.org.

14. The 2009 Stimulus Bill, Electronic Health Records, and Privacy

If you followed the 2008 Presidential campaign, you know that the need for electronic health records was frequently mentioned as a national priority. Not surprising then, the [Stimulus Bill](#), signed by President Obama on February 17, 2009, includes a section on health information technology and [privacy](#). The law allots at least \$19 billion to meet the goal of electronic health records for all Americans by 2014. It also calls for a number of changes to the federal medical privacy rule, commonly known as HIPAA. This federal rule is governed by the U.S. Department of Health and Human Services (HHS).

The new law requires HHS, over the next 18 months, to develop revised rules for, among other things, business associates, rights of patients to restrict disclosures, accounting of disclosures, and notice of a security breach. The PRC will update Fact Sheet 8a as information becomes available. For the best summary currently available, see Privacy and Information Policy Consultant Robert Gellman's, Notes and Observations on Selected Parts of Title XIII, Subtitle D, Privacy, American Recovery and Reinvestment Act Of 2009, Public Law No: 111-5, February 24, 2009, available at: <http://bobgellman.com/rg-docs/Stimulus-Privacy-HIPAA-Analysis.pdf>

The Stimulus Bill is officially called the American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

And the privacy section of the Stimulus Bill is Title XIII, captioned "Health Information Technology," Subtitle D of Title XIII, captioned "Privacy."

15. Tips for Safeguarding Your Medical Information

In reading this guide about the HIPAA Privacy Rule, you may have rightly concluded that your ability to control the flow of your sensitive medical information is limited. Still, the more you know, the better able you are to maximize the privacy you have left.

1. Educate yourself and find out as much as you can about the privacy practices of your health care provider and health plan. Read notices and ask questions if you don't understand.

2. Talk to your provider about your confidentiality concerns. Ask how the provider shares patient data within the office and with affiliates.
3. Remember, you are not just a patient but also a *consumer* of health care. Like any consumer, you can shop for the best privacy deal around. Also, be aware that, as a consumer, you can become a debtor. Unpaid medical bills can be referred to a collection agency or end up as a negative entry on your credit report. The insurance payment process can be complicated and confusing. Be sure to stay on top of your medical bills and dispute matters *in writing* with both the health provider and insurance company when you think errors have been made. Attempt to resolve disputes *before* bills are referred to a collection agency and/or the credit bureaus.
4. Read authorizations carefully. Make your choices about restrictions on authorizations known, and refuse to sign any you are not comfortable with. Keep in mind, authorization forms may ask for your permission to disclose your health information for multiple purposes. One type of authorization is the use of your medical data for marketing. You may withdraw your authorization if you later decide you made the wrong choice.

Because HIPAA authorizes so many different types of disclosures without patient approval, you should be suspicious anytime that someone asks you to sign an authorization form for disclosure of health information. Make sure that the authorization is for your benefit and not someone else's.

5. Exercise your right to obtain a copy of your medical records . Make sure information is accurate. Request that incorrect information be corrected or amended. Keep in mind, your health care provider has the final word on changes and amendments to health records. See the sample letter for requesting a copy of your medical records, www.privacyrights.org/Letters/medical2.htm
6. **Keep a personal health record.** This may include copies of your medical files and other information related to your health such as diet and exercise programs. For more on keeping a personal health file, see the PRC's Alert www.privacyrights.org/ar/keepmedfile.htm and the American Health Information Management Association resources on personal health files. www.myphr.com/what/index.asp.
7. Request that communications be made in a way that you choose. For example, you can request that you be called at your cellular telephone number rather than home phone, or that mailings be sent to your P.O. Box rather than your residential address.
8. Complain if you feel your rights have been violated or your concerns have been ignored. You can file a complaint with both the provider and the Office of Civil Rights. Many problems can be resolved by going directly to the health care provider before you contact DHHS.
9. Contact your representatives in Congress and in your state legislature if you feel stronger laws to protect your medical privacy are needed.
10. Remember that the HIPAA Privacy Rule is new to record keepers, and many providers and insurers are struggling to implement the Rule. Stand up for your rights and let everyone know that you are concerned about privacy, but demonstrate patience and understanding. It will take a lot of effort and time before there is

universal compliance with the HIPAA Privacy Rule.

A final word about complaints: Registering your complaint with your health care provider, the Office of Civil Rights, and your legislative representatives might not result in immediate change. But by complaining, you are educating others about situations that you feel violate your privacy. You are also alerting lawmakers about deficiencies in health privacy law. You are not likely to see changes overnight, but if enough people communicate their dissatisfaction, we might see improvements in the future.

See PRC Fact Sheet 8 for additional privacy protection tips outside the HIPAA arena, www.privacyrights.org/fs/fs8-med.htm.

Sample Letter for Requesting Copy of Medical Files

- www.privacyrights.org/Letters/medical2.htm

16. References and Resources

Filing Complaints under HIPAA

U.S. Department of Health and Human Services (HHS)
Office of Civil Rights
200 Independence Avenue, S.W.
Washington, D.C., 20201
(866) 627-7748

www.hhs.gov/ocr/hipaa

For the regional office nearest you, www.hhs.gov/ocr/hipaahealth.txt

Or email: OCRComplaint@hhs.gov

State Laws and Health Privacy

- Summary of health privacy laws of all states: Health Privacy Project
www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm
- State laws on access to medical records: Georgetown University Center on Medical Record Rights and Privacy, <http://hpi.georgetown.edu/privacy/records.html>
- National Association of Insurance Commissioners (NAIC) - State HIPAA contacts
www.naic.org/state_contacts/docs/hipaareps.pdf
- State Medical Boards
www.ama-assn.org/ama/pub/category/2645.html
- California Office of HIPAA Implementation
www.ohi.ca.gov/state/calohi/ohiHome.jsp

The Patient as Consumer - Credit and Collection Laws

- Fair Debt Collection Practices Act
www.ftc.gov/bcp/online/pubs/credit/fdc.htm
- Fair Credit Reporting Act
www.ftc.gov/bcp/online/edcams/fcra/index.html
- Disputing credit report errors
www.ftc.gov/bcp/online/pubs/credit/crtdis.htm

- Insurers and credit reports
www.ftc.gov/bcp/online/pubs/buspubs/insurers.htm
- Privacy Rights Clearinghouse Fact Sheet 6, "How Private is my Credit Report,"
www.privacyrights.org/fs/fs6-crtdt.htm

Health Privacy Project

- Web: www.healthprivacy.org
- "What You Can Do to Protect Your Privacy,"
www.healthprivacy.org/usr_doc/Checklist.pdf

World Privacy Forum

- Patient's Guide to HIPAA. www.worldprivacyforum.org/hipaa/index.html
- Web page, medical privacy resources: www.worldprivacyforum.org/medical.html

HIPAA Advisory, Phoenix Health Systems

- HIPAA FAQ, www.hipaadvisory.com/action/faqs/faq_main.htm

American Health Information Management Association (AHIMA)

- "Your Health Record," www.ahima.org/consumer/index.cfm
- Analysis of the HIPAA Privacy Rule, www.ahima.org/dc/FinalRulePrivacy.pdf

Emerging Issues Regarding National Health Information Network

Government resources:

- U.S. Dept. of Health & Human Services (HHS) 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

Department of Health and Human Services web site on HIPAA

- The HHS HIPAA page provides links to the Privacy Rule, the Security Rule, and important information for consumers, www.hhs.gov/ocr/hipaa.
 - You can find answers to frequently asked questions about the following topics and more at the DHHS web site. answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php. Or, go to the HHS Home Page, www.hhs.gov, select "Questions" in the top right corner.
- | | |
|-----------------------|--------------------------------------|
| • Authorizations | • Privacy Rule: General Topics |
| • Business Associates | • Protected Health Information |
| • Compliance Dates | • Public Health Uses and Disclosures |

- Covered Entities
- Disclosures for Law Enforcement Purposes
- Disclosures Required by Law
- Facility Directories
- Incidental Uses and Disclosures of Protected Health Information
- Marketing
- Minimum Necessary Standard
- Notice of Privacy Practices
- Personal Reps - Parents and Minors
- Research Uses and Disclosures
- Right to an Accounting of Disclosures
- Right to Amend Medical Records
- Right to File a Complaint
- Right to Restrict Uses and Disclosures
- Right to Access Medical Records
- Safeguards
- Treatment, Payment and Health Care Operations
- Workers Compensation Disclosures

We acknowledge the assistance of privacy consultant Robert Gellman <bob@bobgellman.com> in the preparation of this guide.