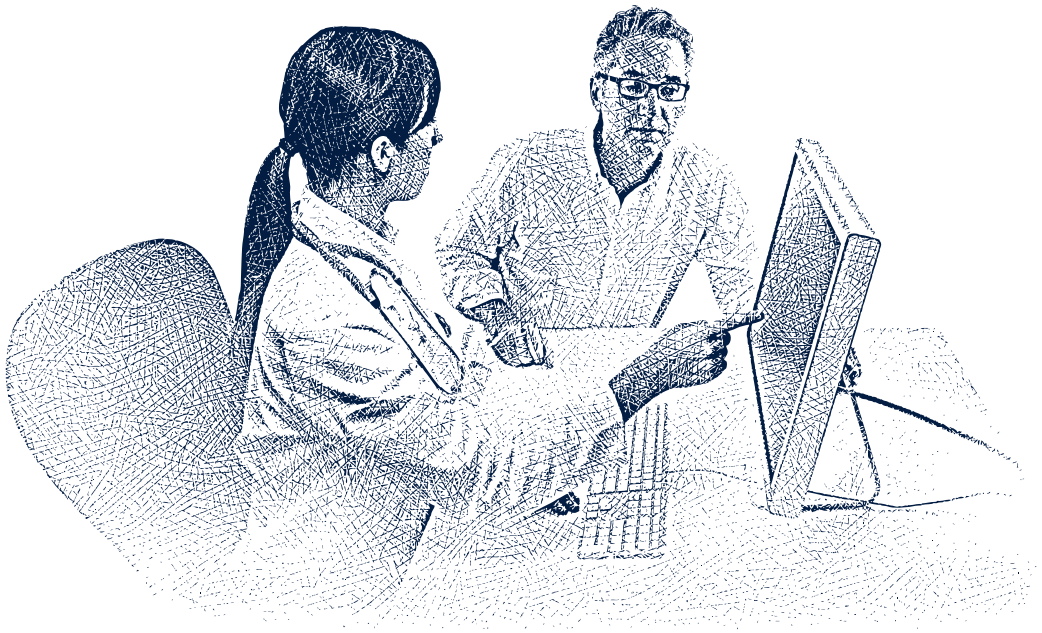
Leader's Guide

Health Records Privacy in California



Answers to Frequently Asked Questions

A Consumer Action Educational Module
www.consumer-action.org/modules

Consumer Action created this brochure under a grant from the Rose Foundation. Consumer Action empowers low- to moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy.

Health Records Privacy in California

Answers to Frequently Asked Questions

Table of Contents

Introduction

Health records contain some of the most sensitive information about us, including details about who we are, how our medical bills are paid and what kinds of medical treatment and diagnoses we've had. For this reason, lawmakers have created rules that help keep patient records private and secure. With the transition to digital health records and the electronic sharing of patient information, there are new potential privacy risks as well as new laws and consumer rights that all patients should be aware of.

When used in conjunction with the multilingual "Health Records Privacy in California: Protecting your privacy as personal health information goes digital" brochure, this backgrounder can help answer many questions about patient privacy rights in the state. The brochure is available in Chinese, English, Korean, Spanish and Vietnamese. For community trainers, there is also a lesson plan, a companion PowerPoint slide presentation and a group learning activity.

The brochure and other materials in this module are free for individuals, non-profits and community-based organizations. For more about these materials, visit the Consumer Action Privacy Information website at www.privacy-information.org. For materials and information on other topics, from money management and credit to housing and insurance, visit www.consumer-action.org or call Consumer Action at 800-999-7981.

Electronic health records

What information do my electronic health records contain?

Regardless of the format—paper or electronic—all patient records contain:

- identifying information such as mailing address, phone number, email address, birth date, account number, family relationships, gender, and race or ethnicity;
- payment information such as billing history, insurance coverage and, in some cases, credit card number; and
- health-related information, including medical history and conditions, medication allergies, family's medical history, office visits, lab results, diagnoses, X-rays and other types of images, referrals to other medical professionals, prescriptions, lifestyle details (such as smoking and alcohol use), psychotherapy and other provider notes, sexual history and more.

Where does the information in my health records come from?

The information in your health records comes from two main places:

- from you, through information you have provided on forms you've filled out—for example, on intake forms when seeking treatment; and
- from your health care providers—each doctor, nurse, pharmacist and other provider that contributes to your treatment enters notes, test results, etc. in your file.

Do all health care providers use electronic health records?

No, not all doctors, pharmacies and other health care providers have converted to electronic health records or are able to exchange patient information electronically. But most of those who haven't done so yet will make the transition by 2015.

Is my health information more vulnerable if it is in electronic format?

Electronic records of any sort are at some risk for a breach—unauthorized access as a result of things like hacking, a lost laptop or mobile device, or a technical error. But paper files are not risk free, either. Documents could be viewed by an unauthorized person, get faxed to the wrong number or get lost in the mail, and they are more likely to be misplaced or damaged.

Because there is the potential for more people to view records held and shared electronically than records kept in a file cabinet, there are restrictions on how electronic records are handled. Various laws and guidelines require health care providers and their business associates to take steps such as encrypting files (making them unreadable to unauthorized viewers), requiring passcodes for file

access and tracking who views files to ensure that electronic patient records remain private and secure.

How do I know my health information is protected when it's being shared electronically?

Large health care providers have the technology to passcode-protect and encrypt patient information themselves. Many independent practitioners and smaller facilities must use a health information organization (HIO) to exchange patient data. In either case, the law requires all parties sharing information to have certain privacy and security tools and procedures in place to protect your information while it's being exchanged.

What if I don't want my health information to be shared electronically?

Most providers who use a health information organization (HIO) to exchange patients' data will ask for your consent (permission) to send your information through the HIO (unless the health information organization does not have access to personal data). Consenting to having your information accessed or exchanged through an HIO does not mean you are giving permission for different or additional uses and disclosures of your information—these remain the same regardless of whether your records are sent electronically, by fax or in the U.S. mail.

If you do not want your information to be exchanged electronically, select that option on the consent form. Or, you can discuss your concerns with your provider directly. Even if your information is not exchanged electronically, your provider is not required to stop maintaining your records in digital format.

Telling your health care provider that you do not want your information shared electronically means that it would not be immediately available to providers who don't routinely treat you and already have your information in their own files. In some cases, emergency room physicians can obtain your information if it is needed to treat you.

What is a personal health record (PHR)?

A personal health record (PHR) is different from an electronic health record (EHR). They are both digital records of your medical information, but an EHR is compiled, managed and owned by your health care provider. Your provider may give you access to some of the information in your electronic health record (your appointment history, physicians list, lab results, prescriptions, immunizations, preventive health reminders, allergies, etc.) via a Web portal (a secure section of the provider's website that you must log in to). Patients can make appointments, email their doctors, renew prescriptions, view lab results and carry out other basic health-related tasks online. But you cannot add or change the information, and you can't transfer it to a new provider. The data contained in your records

held by your health care provider is subject to federal and state health information privacy rules.

Personal health records often are offered by non-HIPAA covered entities. PHRs are compiled, managed and owned by you, the patient. You can add any medical information you want, change it as needed, and share it with anyone you choose. PHRs enable you to access your essential medical information from any place at any time (usually via the Web or a USB/Flash drive). This can be useful for travelers and also if you're seeing multiple providers who don't have access to the same database. When you create your personal health record, you can include information from your medical records as well as additional information, such as your eating habits and exercise routine. There may be a fee or subscription cost for maintaining your PHR, and your privacy rights will be based on the company's own policies and any other applicable laws, not on HIPAA.

You can learn more about PHRs at MyPHR.com (www.myphr.com).

Health information privacy laws

What is HIPAA and how does it protect me?

HIPAA, short for Health Insurance Portability and Accountability Act, is the main federal law that governs how patients' protected health information (PHI) is collected, used and disclosed.

All "covered entities" (providers and businesses covered by HIPAA) must comply with the law *unless* state laws provide stronger protections for patients—then they must comply with the stronger state law.

The World Privacy Forum offers an in-depth yet easy-to-read guide to HIPAA (http://www.worldprivacyforum.org/hipaa/guidecontents.html).

What is a "covered entity"?

A covered entity is an individual or business that must comply with HIPAA rules. Generally speaking, covered entities include:

- health care providers (for example, doctors, hospitals, pharmacists, laboratories, dentists, and specialists such as podiatrists and optometrists);
- health plans (for example, health insurers, health maintenance organizations (HMOs) and programs such as Medicare);
- health care clearinghouses, which are businesses that transmit claims, billing data and similar types of information; and
- business associates, which create, receive, maintain or transmit patient information for a covered entity.

Providers that might not be covered by HIPAA include services like:

- free clinics;
- a first-aid room at your workplace; and
- health screening services you participate in at places like the mall or local drugstore.

If you don't know if a provider or business is a HIPAA covered entity, ask.

California law applies to some health care services that may not be covered under HIPAA. These include primary care clinics (community clinics and free clinics) and specialty clinics, emergency centers, skilled nursing facilities, correctional treatment centers, hospices, home health agencies, intermediate care facilities, mobile health care units and acute psychiatric hospitals.

What is protected health information (PHI)?

PHI is any information held by a HIPAA covered entity that is related to your health status, medical treatment or payment for health care services that can be linked to you personally. California law typically refers to this as "individually identifiable information." It is this type of information that federal and state laws protect.

How does the HIPAA Privacy Rule protect me?

The HIPAA Privacy Rule requires covered entities to use safeguards to protect the privacy of your health information and sets limits and conditions on how your information can be used and disclosed. It applies to your protected health information in any format, not just electronic.

The Privacy Rule also gives you a number of rights, including the right to:

- inspect or obtain a copy of your health records and request corrections;
- know how your information has been disclosed for other than routine treatment, billing and related purposes; and
- request that you be contacted by your provider or health plan in a particular way (for example, at your cell phone number instead of your home or work number or via email rather than by postal mail).

How does the HIPAA Security Rule protect me?

The HIPAA Security Rule applies specifically to electronic records. It requires covered entities to use safeguards to ensure the confidentiality and security of your information held in digital format. These safeguards include:

- ensuring that third-party contractors or vendors comply with HIPAA;

- properly disposing of equipment and data so that patient information remains confidential;
- limiting access to information to only authorized individuals; and
- encrypting patient information that is transmitted electronically.

Recent changes to the Privacy and Security Rules require, among other things, that:

- you be notified if your unencrypted health information has been breached (accessed without authorization);
- you receive a Notice of Privacy Practices (NPP) that makes clear that your authorization is required for most uses and disclosures of your protected health information for marketing purposes;
- your written permission be obtained before your information can be used or disclosed in ways not described in the Notice;
- you be allowed to opt out of fundraising communications; and
- your request to withhold disclosures to a health plan be honored if you pay for the health services or items out of your own pocket.

Will my health records be protected if my provider or another entity covered by HIPAA transfers my records to an entity not *covered by HIPAA?*

No. Once your records are in the hands of an individual or business that is not considered a covered entity under HIPAA, the law does not apply. The privacy of your health records would be governed either by other laws that apply, which may be stronger state laws, or by the privacy policy of the recipient. For this reason, it's very important to be careful about giving your information or authorizing the transfer of your information to anyone not directly involved in your medical treatment or payment for your health care.

Are there stronger health information privacy laws in California?

In some cases, yes. The Confidentiality of Medical Information Act (CMIA) is the main California law that protects the privacy of residents' medical information. It gives patients even stronger rights than HIPAA provides in many cases. And it applies to more types of providers, such as hospices, clinics, home health agencies, intermediate care facilities, mobile health care units and acute psychiatric hospitals.

Use and disclosure of health records

What is the Notice of Privacy Practices I received from my doctor?

Your health care provider and health plan must give you the Notice of Privacy Practices, which explains how they are allowed to use and disclose your health

information and how you can exercise your health privacy rights. Your information cannot be used or disclosed in any way that is inconsistent with the Notice unless you provide your written permission ("consent" or "authorization").

If you did not receive the Notice on your first office visit or in the mail, you can ask for a copy or visit the website of your plan or provider to get it.

What is the difference between consent and authorization?

Under both state and federal the law, a physician can use and disclose your health information for treatment, payment or health care operations (things like auditing, resolving complaints and evaluating quality of care) without your written permission. For other uses and disclosures of your information, your written permission is required. Under HIPAA, this is referred to as your "authorization," while "consent" under HIPAA refers to permission that is requested but not legally required.

California does not distinguish between "consent" and "authorization" the way HIPAA does, but the rules under state law are the same: Your written permission is *not* needed for routine uses of your information by your health care providers (except in some cases when the information being used or disclosed is deemed particularly "sensitive") but it *is* needed for most other uses if they are not allowed or required by law.

What if I don't sign the Notice of Privacy Practices?

Your health care provider may ask you to sign the Notice of Privacy Practices as proof you received it, but your signature is not required. Signing the Notice won't change or waive your rights, and it doesn't mean you have agreed to any special uses or disclosures of your health information.

You can't be denied access to a physician because you don't sign the Notice.

If I make a change to the Notice of Privacy Practices or an authorization form, is it still valid?

Making a change on the Notice of Privacy Practices will have no impact as it is only used to inform you of how your health information can be used or disclosed under the law and what your rights are.

If you choose to sign an authorization form but disagree with some part(s) of it, cross out and change the text you don't agree with and initial the change.

Who has automatic access to my health records without my written permission?

Your health care providers, health plan and those who pay for your care have a right to use and disclose your health records as needed to administer treatment,

process claims and manage their health care operations. They do not need your written permission (“consent” or “authorization”).

Those who pay for patient care include insurance companies, Social Security disability, Medicare, Medicaid, workers compensation funds and the Department of Veterans Affairs. It may also include your employer if your employer helps fund your medical care, but there are some limits to what information your employer has access to and rules about how it must be protected.

Are there situations when my information can be used or disclosed without my written permission?

In addition to treatment, payment and health care operations, your information can be used or disclosed without your permission for the following purposes:

- law enforcement (for example, when blood type is needed for an investigation, or if you are incarcerated);
- public health activities (related to infectious disease control or recording births and deaths (coroner), for example);
- to report abuse, neglect or domestic violence;
- health oversight activities (such as an audit);
- to communicate with a family member or other person involved in your care in an emergency or when you can’t speak for yourself;
- legal proceedings (such as a court order or subpoena);
- special government functions (such as military or national security);
- workers’ compensation claims;
- workplace medical surveillance or handling of a work-related illness or injury;
- some types of research (your name cannot be released to the public, and patient information is often “de-identified,” or made anonymous);
- to identify someone who has died, determine cause of death, etc.;
- organ donation; and
- collecting on unpaid medical bills.

How much of my information will my health care provider share?

Health care providers are supposed to disclose to non-health care entities only the minimum information needed for the particular purpose ("minimum necessary" guideline)—not your entire health record. Ask how your provider ensures that only pertinent information is shared.

What uses of my information require my written permission?

Your written authorization or consent is required for any use or disclosure of your protected health information (or individually identifiable information) outside of legally permitted purposes (treatment, payment, health care operations and other uses listed above). That includes many marketing scenarios, some research projects, and disclosures to some third parties.

Certain types of health information are subject to additional legal protections. These include:

- HIV test results and AIDS status;
- alcohol and drug treatment records;
- mental health status/psychotherapy notes; and
- genetic test results.

These additional protections often include a requirement for your separate signed authorization for each release of the information—in some cases, even for the purpose of treatment. Any covered entity that exchanges sensitive patient information must be able to comply with the additional requirements in the format they are using (paper or electronic).

What information must a valid authorization contain?

To be valid, an authorization must include (in addition to your identity):

- a description of the health information to be used or disclosed;
- the person or entity authorized to use or disclose the information;
- the person or entity authorized to use or receive the information;
- an expiration date or event (such as, when you are no longer enrolled in the plan); and
- in some cases, the purpose for which the information may be used or disclosed.

What happens if I don't give my authorization?

That depends on the situation. For example, authorization is typically required when you apply for some types of insurance (health and life, for example). In this case, refusing to authorize the release of your medical information most likely would result in your application being declined. Likewise, if your authorization is required to participate in a medical research study, you probably wouldn't be allowed to participate without it.

A health care provider isn't allowed to withhold treatment from a patient who doesn't sign an authorization.

Will my health care provider release my information without my authorization?

Medical providers will not release your records to a third party not directly involved in your treatment, related billing or other health care administrative functions without your authorization unless allowed or required to do so by law—and then the information disclosed should be limited to the minimum required for the purpose.

How can I cancel my consent or authorization if I previously gave it, or give it if I previously denied it?

Contact your provider for instructions on how to change your selection. You most likely will have to fill out a new form.

Can I find out who has accessed my health records?

You can request an "accounting of disclosures," which will tell you everyone who has received your health records for the past six years for purposes *other than* treatment, payment and health care operations.

Does the accounting of disclosures include every instance of my health records being shared?

There is a proposal to change the accounting of disclosures requirement to include *all* disclosures of your personal health information, including those made for purposes of treatment, payment and health care operations, for three years prior to the date of your request. But until that proposal is adopted (if ever), the accounting only includes disclosures for purposes *other than* treatment, payment or health care operations for the past six years.

When can—and can't—my health information be used for fundraising purposes?

Under HIPAA, fundraising is considered a health care operation. As such, a covered entity is allowed to use or share your demographic and contact information and appointment dates, but not your treatment information, without your permission to fundraise for the institution's own benefit. California does not have a law governing fundraising.

A fundraising communication must allow you to opt out of future fundraising communications. However, the fundraiser only has to use "reasonable efforts" to comply with your request.

When can—and can't—my health information be used for marketing purposes?

In California, a covered entity needs your written permission before it can use or disclose your health information for marketing purposes, and it must notify you of how the information could be used and shared.

However, your information *can* be used for marketing *without* your authorization if the marketing message concerns your health plan's services, benefits or more cost-effective products; if the message is tailored to you and tells you about other treatment options; or if the sender is not paid for delivering the message. If the sender has been paid, it must say so, and it must give you the ability to opt out of future communications.

If you take part in free or low-cost health screenings (often at pharmacies, health fairs and malls), sign up for store discount cards that record what you purchase, use health-related mobile apps, participate in online medical forums, etc., you may be willingly revealing your information to marketers without even realizing it. Read any authorization forms you are asked to sign very carefully.

Access to health records

Can I see my own medical records?

Yes, you have the right to access your medical records upon written request to your doctor. The doctor must allow you to view your records on-site during business hours within five business days of your request. Copies must be provided within 15 days of request, or 10 days if you agree to receive a summary. If the provider needs more time to provide the summary, s/he can take up to 30 days as long as you are notified and told when the summary will be ready. Copies of X-rays and similar records don't have to be provided to you if they are transmitted to another provider within 15 days of your written request.

You have the right to receive an electronic/digital copy of your records if they are available in that format, and to have it sent to another person or provider you choose.

Can I be charged for obtaining a copy of my records?

In California, providers are allowed to charge up to 25¢ per page for photocopies or 50¢ per page for copies from microfilm, along with "reasonable" clerical costs for making your records available to you. If you get a summary of your records, the provider can charge a "reasonable fee" based on the actual time and cost to prepare it.

There is no charge for a copy of the relevant part of your medical records if you need the information to appeal a denial of eligibility for public benefits, such as Medi-Cal or Social Security. But you can be charged for the copy if you win the appeal.

Can I be charged for viewing my records at my provider or health plan's office?

California law allows providers to charge for "clerical costs incurred in making the records available" to you. This means that it is possible you will have to pay a fee.

Does my doctor have to send a copy of my records to another doctor if I request it?

No, although many providers transfer records as a courtesy if you sign an authorization form approving the release of your information.

Since provider-to-provider records transfers are not required under the law, there is no time limit for transferring patient records and no penalty for failure to do so. If you're having trouble accomplishing the transfer, you could request a copy of your records for yourself. There may be a charge for this (see above), but the doctor has to get the copy to you within 15 days. You can then provide a copy of your records to anyone you choose.

Can my provider withhold my records?

Yes, but only in the case of mental health records. Your provider might refuse your request to see or copy your mental health records if s/he determines there is a substantial risk of harm if you are given access. If that is the case, the provider must add to your record the date of your request and the reason it was denied. These notes must include a description of the specific negative results that the physician believes would occur if you were allowed to see your records. Your records cannot be withheld just because the provider believes they could upset you.

Health care providers are prohibited from withholding patient records because of unpaid bills.

Can I make changes to my health records?

You have the right to ask your provider to amend (change) your records to make them more accurate or complete. The provider must act on your request within 60 days, though s/he can have a 30-day extension as long as you receive a written notice of the delay and the reason for it, as well as the date by which your request will be handled.

Can a provider deny my request for changes to my health records?

The provider can deny your request to change your records if s/he believes that the information is accurate and complete, if s/he did not create the record or does not have the record, or if you don't have the right to access the record.

If your request is denied, you must be given the reason. You have the right to provide a written statement of up to 250 words regarding anything in your records that is incorrect or incomplete. The provider must add the statement to your records and include it whenever a disclosure of the information you believe is incorrect or incomplete is made to any third party.

What can I do if my provider won't give me access to my health records, charges me too much for copies or won't let me amend my records?

If you believe your provider is not following regulations, you can file a complaint with the California Medical Board (http://mbc.ca.gov/consumer/complaint_info.html), which is responsible for investigating complaints and disciplining health care professionals. You can also file a complaint against a HIPAA covered entity with the federal Department of Health and Human Services Office for Civil Rights. (See companion brochure for contact information or visit http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.)

You have the right to sue in California Superior Court to protect your rights under California law. For example, you can sue for access to your medical information, have records retrieval fees reduced if you think they are unreasonable, or get your statement added to your file. The judge can award court costs and lawyer's fees to the side that wins the case. You do not have the right to sue your health care provider for these issues in federal court.

Do my family members have access to my medical records?

Health care providers are not prohibited from discussing your health and treatment with your family members or from allowing them to pick up your prescriptions, but they need your signed authorization before they can release your medical records to anyone. If you want someone close to you to be able to access your records, you can designate a "personal representative." Ask your provider for the necessary form.

When might my employer have access to my health records?

HIPAA prohibits health care providers, health plans and other covered entities from disclosing your health records or information without your written authorization unless other laws require they do so. That includes most disclosures to your employer.

However, a provider could disclose patient information related to a job-related injury or illness or workplace medical surveillance. (Medical surveillance is the monitoring of workers' health for the early detection of possible adverse effects of a particular job, materials, etc.). And HIPAA does not prevent your employer from asking you for a doctor's note or other information about your health if it is needed to administer sick leave, workers compensation, family and medical leave, wellness programs or health insurance, you have asked for a change in job duties for health reasons, or you are required to pass a drug test for your job. It also does not protect your confidentiality when you have raised your health as an issue in a work-related dispute.

Some large employers are self-insured. While these employers may have access to some of the personal information in your records, it is generally not sensitive

medical information. In California, the law requires employers who receive your medical information to protect its confidentiality and to get your authorization before disclosing any of it.

The U.S. Department of Labor (www.dol.gov) provides information about the privacy of employee medical information in the workplace.

I'm in the military—does my commanding officer have access to my health records?

The records of military members are protected (or not protected) in virtually all the same ways as civilian records. The one main difference is the following, excerpted from https://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/hipaamil.html:

"In order for a commander to know which subordinates are mentally and physically able to serve and deploy to fight, the commander is permitted access to the information in the subordinates' medical and mental health records….The MHS [Military Health System] can disclose PHI to a commander to determine the member's "fitness for duty" and "fitness to perform any particular mission, assignment, order, or duty."… When disclosing PHI in any form, the MHS must make "reasonable efforts" to limit the use or disclosure of PHI to "the minimum necessary" to accomplish its intended purpose."

The "minimum necessary" guideline is the same as for civilian records. But, of course, civilian employers don't have such access to employees' medical and mental health records.

Medical and prescription reporting agencies

What is the MIB and what information does it collect?

Specialty consumer reporting agencies are similar to credit reporting agencies, but they compile very specific information about things other than your credit use or bill payment history. The Medical Information Bureau (MIB) is one such specialty consumer reporting agency. Insurance companies use MIB reports to evaluate applicant risk.

An individual's MIB report includes:

- medical conditions;
- medical tests and results;
- high-risk lifestyle choices or addictions (smoking, taking drugs, overeating, etc.);
- dangerous activities (rock climbing, skydiving and traveling to places considered unsafe, for example);

- motor vehicle reports (poor driving history and accidents);
- credit information; and
- requests for your file in the previous 12 months.

Information stays in your file for seven years.

The MIB is the largest medical information reporting agency, though it has reports on only a fraction of consumers. If you have not applied for an "individual" (as opposed to "group") life, health, long-term care, critical illness or disability policy during the last seven years, you will not have an MIB report.

Specialty consumer reporting agencies are subject to the Fair Credit Reporting Act (FCRA) and, as such, have to follow the same rules that credit reporting agencies do. That includes providing you with one free report every 12 months upon your request, allowing you to dispute inaccurate and outdated information, and making corrections if warranted.

Request your MIB report at 866-692-6901 or online at http://www.mib.com/facts_about_mib.html.

What are prescription reporting databases?

MedPoint and IntelliScript are the names of the two main prescription reports. Prescription reports reveal what medications you've used over the past five years, the dosages, when you refilled the prescriptions and your physician visits.

Request your MedPoint file at 888-206-0335. Request your IntelliScript file at 877-211-4816 or online at http://www.rxhistories.com/contact_us.html.

How do the MIB, IntelliScript and similar databases get my information?

These companies get much of your information from insurance companies—from an insurance application you filled out or a medical exam you took as part of the underwriting process, or from any records that you authorized be released to them.

Will my insurance provider release my information without my authorization?

Insurance companies are obligated to notify you how they may share your information and allow you to opt out of sharing with third parties. Read authorization forms carefully to understand exactly how the insurer could use your information.

Is my written permission required for someone to access my medical or prescription report(s)?

Yes, you must sign an authorization form before your file can be accessed. According to the MIB privacy policy, the company only shares individually identifiable information with its member life and health insurance companies, and only with your authorization, unless otherwise required or allowed by law. MIB says it does not sell any individually identifiable information to any non-member third parties.

What if the information in my report(s) is wrong?

Under the Fair Credit Reporting Act, you have the same right to dispute inaccurate or expired information in your specialty consumer reports that you have to dispute information in your credit reports. Follow the dispute instructions that come with the report. The reporting agency must complete its investigation of your dispute in a reasonable period—typically within 30 days. If the information is confirmed to be inaccurate or outdated, it must be corrected or removed, and the reporting agency has to send you the results of the dispute.

If the reporting agency confirms that the information is timely and correct, then it will remain. However, you have the right to include a short "statement of dispute" that will be seen by anyone who requests your report. If information is changed or removed, or if you add a statement, you can request that anyone who recently received your report be notified of the change.

To file a complaint against a consumer reporting agency, contact the Federal Trade Commission (FTC) (https://www.ftccomplaintassistant.gov/; 877-FTC-HELP) and the Consumer Financial Protection Bureau (CFPB) (www.consumerfinance.gov; 855-411-2372).

Data breaches, medical identity theft and fraud

Will I be notified of a data breach?

California law requires any company that collects personal information to notify all California residents in its database if there is a breach of their *unencrypted* personal information, including medical and health insurance information.

The notice must include the date and time of the breach, a general description of the incident, and the types of information at risk. It also must include the toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California ID card number.

You can view or search a list of data breaches on the California Attorney General's website (http://oag.ca.gov/ecrime/databreach/list).

What should I do if I'm notified that my information has been breached?

That depends on what parts of your personal information have been accessed. Read Privacy Rights Clearinghouse's "Fact Sheet 17b: How to Deal with a Security Breach" (https://www.privacyrights.org/fs/fs17b-SecurityBreach.htm) to find out what steps to take to protect yourself after the incident. These steps might include filing a police report, monitoring your credit reports, using a fraud alert, or notifying your creditors, health care providers, medical insurance provider and others.

What is medical identity theft?

Medical identity theft occurs when someone steals your personal information—often your health insurance account number, your Medicare or Medi-Cal number or your Social Security number—and uses it to obtain health care, prescriptions and other medical services in your name or make false insurance claims for medical goods and services. Your medical coverage information can be stolen in a variety of ways, including directly from your medical records, from a form you fill out, or from ID cards you keep in your wallet.

What are the possible repercussions of medical identity theft?

The repercussions of medical identity theft can be very serious:

- Your health care provider could treat you for a disease you don't have, prescribe a medication you are allergic to, not prescribe a necessary medication because your records mistakenly show you are already taking it, or give you the wrong blood in a transfusion because your record reflects the identity thief's blood type.
- You could be denied insurance coverage (life or long-term care, for example) because the underwriter believes you have a serious disease you don't have. Or you could be turned down for a job or promotion because your health record makes it look like you have a medical issue that would not allow you to perform your new job duties.
- You could be asked to pay for medical services that would normally be covered by your insurance because the identity thief has caused you to reach the coverage limit under your policy.
- You could be contacted by collectors because the identity thief has run up unpaid medical bills. Your credit score could be damaged, leading to declined loan applications or higher interest rates when you borrow.

What are the signs of medical ID theft?

Some signs of medical identity theft are:

- medical bills for services you have not received;
- calls from collectors about medical bills you don't recognize; and

- being told you've reached your medical insurance coverage limit even though you don't believe you have.

How can I prevent medical identity theft?

You can reduce the chances of becoming a medical identity theft victim by taking some precautions:

- Keep health care records, insurance statements, bills and other medical paperwork filed in a safe place, and shred what you don't need to keep.
- Review all medical bills, the insurance "explanation of benefits" you receive after each visit or claim, and any other paperwork related to your medical treatment and health insurance carefully to be sure you were the one to receive all the services, treatments, prescriptions, tests or supplies described. Contact the health care provider or your health plan or insurance company to go over anything that looks inaccurate.
- If possible, try to avoid giving out your Social Security number, or try to limit it to the last four digits.
- Don't give out your sensitive information in exchange for "free" medical services, tests, drug samples, etc.

What should I do if I'm a victim of medical identity theft?

The Federal Trade Commission (http://www.consumer.ftc.gov/articles/0171-medical-identity-theft) and the World Privacy Forum (http://www.worldprivacyforum.org/medidtheft_consumertips.html) both offer detailed information about dealing with medical identity theft, from filing a police report or Identity Theft Affidavit to removing erroneous information from your medical records.

Assistance and information

See the "Health Records Privacy in California: Protecting your privacy as patient records go digital" brochure for information about where to file a complaint if you believe your privacy rights have been violated. The following are resources that provide additional information about your health records privacy rights.

California Attorney General's Office (http://oag.ca.gov): In addition to taking privacy complaints, the AG's office offers a "Consumer Guide to Health Information Privacy in California" (http://oag.ca.gov/privacy/facts/medical-privacy/patient-rights) on its website.

California Office of Health Information Integrity (CalOHII) (www.ohii.ca.gov/calohi): Site visitors will find extensive information about California medical privacy laws and enforcement. The "Patient FAQ" (www.ohii.ca.gov/privacy360/Patients/PatientFAQ.aspx), "Provider FAQ"

(www.ohii.ca.gov/privacy360/Providers/ProviderFAQ.aspx) and “Individual’s Rights to Medical Information Privacy-FAQs” (http://www.ohii.ca.gov/calohi/MedicalPrivacyEnforcement/ReportingViolation/FAQs.aspx) pages are particularly helpful.

California Patient’s Guide (www.calpatientguide.org): Prepared by Consumer Watchdog, the guide includes a section on medical records and confidentiality.

Georgetown University's Center on Medical Record Rights and Privacy (http://hpi.georgetown.edu/privacy/records.html)**:** Offers guides on medical records privacy laws and patient rights in all states.

Medical Board of California (http://www.mbc.ca.gov): Among other topics, the California Medical Board’s website includes pages on patient access to medical records (http://www.mbc.ca.gov/consumer/access_records.html) and related questions and answers (http://www.mbc.ca.gov/consumer/complaint_info_questions_records.html).

Privacy Rights Clearinghouse (www.privacyrights.org): Offers a large online library of materials on medical privacy (https://www.privacyrights.org/Medical-Privacy) and electronic health records exchange, some of it California-specific.