How Is Your Medical Information Used and Disclosed? (California Medical Privacy Series) [1]

1. **What does this guide cover?**

2. **What information is in your medical records?**

3. **Do you own your medical records?**

4. **Where can you learn about a health care provider or health plan’s privacy practices?**

5. **Can you choose how your medical information is used and disclosed?**
   a. **Authorization versus consent**
   b. **Before you sign an authorization form**

6. **When do health care providers and health plans need your authorization (written consent) to use or disclose your medical information?**
   a. **Authorization to use or disclose sensitive information**
   b. **Authorization for research**
   c. **Authorization for marketing use and sale of medical information**

7. **When can health care providers and health plans use or disclose your medical information without your authorization or consent?**
   a. **Mandatory disclosures**
   b. **Medical treatment**
   c. **Payment**
   d. **Health care operations**
   e. **Contractors/business associates**
   f. **Others involved in your care**
   g. **Government agencies and law enforcement**
   h. **Employers**
   i. **Insurers**
8. **Can your health information be used or disclosed outside the healthcare context without your authorization or consent?**

9. **Resources**

1. **What does this guide cover?**

This guide discusses how healthcare providers and health plans may use and disclose your health and medical information. It would be impossible to list all possible uses and disclosures, but the guide covers many common examples.

2. **What information is in your medical records?**

A typical medical record contains a lot of personal and sensitive information, including:

- Full name and unique identifiers such as a provider account number.
  - Note that many providers have eliminated Social Security numbers (SSN) from patient records because of the risk of identity theft. At minimum, SSNs should be truncated to reveal only the last four digits.
- Contact information including address, phone numbers, and email address.
- Demographic information such as gender, race, and ethnicity.
- A history of medical conditions; prescription allergies; and drug, alcohol, and smoking habits.
- Records of patient visits, diagnoses, treatments, test results, prescriptions, and referrals to other doctors.
- Billing and payment information, such as the party responsible for payment, insurers, and a beneficiary.
- Information patients provide on intake forms about immediate family members such as medical histories.

3. **Do you own your medical records?**

No. Medical records are the property of the medical provider (or facility) that prepares them. As a patient, you have a right to view the originals, and get copies. Cal. Health & Safety Code §§ 123100 - 123149.5 [2].

4. **Where can you learn about a health care provider or health plan’s privacy practices?**

Healthcare providers and health plans are required to develop and distribute a notice of privacy practices explaining how they may use and disclose protected health information.

Healthcare providers and health plans must make the notice available on any website they maintain and provide it to anyone who asks. Health care providers typically post the notice at the office or provide a copy at your first visit. Health plans provide the notice when you enroll in an insurance plan.

These notices can provide you with valuable information, including:

- how the provider or plan may use and disclose your medical information;
- your rights and how to exercise them;
- how to complain to your health care provider or plan;
- how to file a complaint with the U.S. Department of Health and Human Services’ Office for Civil Rights (which enforces HIPAA); and
- who to contact for further information about the privacy policy.

A notice of privacy practices is just that – a notice. It is not a consent form. Your signature does not authorize any use or disclosure of your health information. Similarly, refusing to sign a notice of privacy practices does not prevent the provider or plan from using and disclosing your information as stated in the notice.


5. **Can you choose how your medical information is used and disclosed?**

At times, California’s Confidentiality of Medical Information Act (CMIA) generally prohibits disclosure of medical information without authorization. However, there are so many exceptions that it is safer to say you have limited opportunities to authorize or consent.
a. Authorization versus consent

Note that authorization and consent are not interchangeable terms. Authorization is written consent that gives others permission to access and use your medical information. It has a defined legal meaning. CMIA’s requirements for valid authorization are available at Cal. Civ. Code § 56.21 [4]; HIPAA requirements are at 45 CFR § 164.508(c) [5].

b. Before you sign an authorization form

- Make sure you read and understand any authorization form before you sign.
- Question anything you don’t understand or that makes you uncomfortable.
- Be wary if the form authorizes disclosure or use for all legally valid purposes and has no time limit.
- Consider editing the terms or declining to sign the form if you remain uncomfortable.

6. When do health care providers and health plans need your authorization (written consent) to use or disclose your medical information?

a. Authorization to use or disclose sensitive information

California law requires written authorization for use or disclosure of certain types of sensitive information. Note that there are exceptions where authorization may not be required.

Authorization is required for:

- Drug and alcohol treatment records. Cal. Health & Safety Code §§ 11845.5 [7], 123105(b) [8].
- HIV status and test results. These may not be disclosed without written authorization if they contain personally identifiable information and were developed or acquired by a state or local public health agency or its agent. However, there are exceptions. These include disclosure for diagnosis, care, treatment, and mandatory state and federal public health reporting (for example to the California Department of Public Health and the Centers for Disease Control). Employees and contractors of state and local health care agencies that receive individually identifiable information concerning HIV must sign a confidentiality agreement. Cal. Health & Safety Code §§ 121025-121125 [9].
- Genetic test results for a life or disability insurance application. Cal. Ins. Code § 10140.1 [10].

b. Authorization for research

Researchers who want to use identifiable medical information generally need either written authorization or a waiver of the authorization requirement from an Institutional Review Board (IRB).

An IRB is a committee at an institution (such as a hospital or university) that reviews and approves research involving human subjects. IRBs help ensure that research is conducted in accordance with federal, institutional, and ethical guidelines.

Researchers conducting public health research will not need to obtain authorization.

Researchers using de-identified data or a limited data set will not need to obtain authorization.

De-identified data has had 18 specific identifiers removed. 45 CFR § 164.514(b)(2) [11].

A limited data set has had most identifiers removed, but may still include:

- dates of admission or discharge from a hospital;
- dates of medical treatment;
- date of birth and death;
- age; and
- Zip code with state, county, city, or precinct.

c. Authorization for marketing use and sale of medical information

Health care providers, health plans, and their contractors must obtain written authorization prior to using your medical information for marketing purposes. They must also provide you with clear notice about how your information will be used and shared, and tell you whether they will receive payment for sharing the information.
There are exceptions. For example:

- Health plans can communicate to members about plan benefits, plan services, and the availability of cheaper prescription drugs.
- Providers and plans can advise or educate individuals about treatment options. However, they must clearly disclose any payment they are receiving to communicate those options and the source of the payment. They must also give you the ability to opt out of future communications.

For more information about marketing use and sale of medical information, see 45 CFR § 164.508(a)(3) [12]; Cal. Civ. Code §§ 56.05(i) [13] and 56.10(d) [14].

7. When can health care providers and health plans use or disclose your medical information without your authorization or consent?

CMIA generally prohibits unauthorized disclosure of medical information, but there are many exceptions. In some situations health care providers, health insurance companies, and their contractors are required to disclose medical information. Other times they may choose to disclose information. See Cal. Civ. Code § 56.10 [14] for the full list of exceptions. The examples below are not exhaustive, but include many of the ways your medical information may be used or disclosed without your consent or authorization.

a. Mandatory disclosures

Health care providers, insurance companies, and their contractors must disclose medical information when a patient or patient’s representative requests the information, when they receive a court order, in civil and criminal legal proceedings, for many purposes involving death investigations, and when otherwise required by law.

b. Medical treatment

Your medical information can be used and disclosed for the purpose of treating or diagnosing you.

c. Payment

Whoever is responsible for paying your medical bills (such as an insurer, employer, or governmental authority) may receive the information necessary to determine eligibility, treatment fees, and payments due. Insurers can’t see an actual medical record without authorization, but they do receive treatment codes for billing that can provide enough information to create an outline of your medical history.

Debt collection

If you are late paying your bills, a health care provider may hire a debt collector to pursue payment. Under HIPAA, collection agencies may only receive the minimum amount of information necessary to collect the debt. However, this is a subjective determination.

For more information, see:

- HHS/OCR HIPAA and debt collection FAQ [15];
- HHS explanation of business associates [16];
- HHS/OCR guidance on the minimum necessary rule [17].

Credit reports

Consumer reporting agencies (such as credit bureaus) may receive your name and address, date of birth, Social Security number, payment history, account number, and the name and address of the health care provider or health plan. They may not receive specific medical information or billing codes.

Consumer reporting agencies may not include medical information in reports for employment, credit transactions, or insurance transactions without your authorization. A consumer reporting agency may not disclose the name, address, and telephone number of the medical provider responsible for the information in the report. In addition, creditors may not base a decision to grant credit on medical information. See Pub. L. No. 108-159, 117 Stat. 1952 (2003) [18] and Cal. Civ. Code § 1785.13(f) [19].
d. Health care operations

Medical information may be disclosed without authorization for health care operations. The definition is very broad and it is impossible to provide a comprehensive list, but health care operations can include:

- a standards board rating the quality of a health care provider;
- a provider contacting patients about treatment alternatives and related matters;
- training for health care professionals;
- a provider creating, renewing, or replacing health insurance contracts or benefits;
- fraud, abuse, and regulatory compliance audits;
- business management and general administrative duties;
- data transfers involved in the sale, merger, or consolidation of a provider; and
- fundraising (though there are notice and opt-out requirements)

45 CFR § 164.501 [20]

e. Contractors/business associates

Health care providers and health plans often contract with other people or businesses for their services. This means people or businesses with whom you have no direct relationship have access to your health and medical information.

These often include medical groups; independent practice associations (groups of doctors that contract with HMOs); pharmacy benefits managers; and medical service organizations such as businesses that provide practice management and operational services like billing, payroll, employee benefits management, and general administration. These people or businesses may both have access to and the ability to further disclose your medical information without your authorization.

California law uses the term contractor while HIPAA calls them business associates. See Cal. Civ. Code § 56.05(d) [21] and 45 CFR § 160.103 [22] for their respective definitions.

In California, CMIA applies directly to contractors. Additionally, HIPAA requires business associates to comply with many of the same privacy and security requirements that apply to covered entities. For more information about business associates, visit the HHS website [16].

f. Others involved in your care

Your doctor may share health information with your family, friends, and others who are involved with your health care or payment unless you object. However, providers often have their own more restrictive policies. For more information, see the HHS website [23].

g. Government agencies and law enforcement

Claims processing and investigation
State and federal government agencies may request medical records to verify claims. These include Medicare, Medicaid, MediCal, Social Security Disability, and Workers Compensation. In addition, the Office for Civil Rights of the U.S. Department of Health and Human Services can access medical records if investigating a relevant claim.

Prescription drug monitoring
All health care providers and pharmacists must report their prescriptions for Schedule II through IV controlled substances [24] to the California Department of Justice’s Controlled Substance Utilization Review and Evaluation System, better known as CURES [25].

Licensed prescribers and pharmacists may access the database only for their own patients. Law enforcement agencies and CURES staff may access the database for official oversight and investigations. Law enforcement agencies often use the information in CURES to monitor the use and potential abuse of controlled substances. For more information on prescription drug privacy, see California Medical Privacy Guide: Prescriptions and Your Privacy [26].

Public health reporting
Public health authorities may receive personal health information without your authorization for the purposes of preventing or controlling disease, injury, or disability.

Examples include:
monitoring epidemics;
food, drug, and radiation safety;
environmental and occupational disease control;
reporting on specific diseases (California Department of Public Health has a list available here [27]);
child and elder abuse;
reporting births and deaths;
intervening in emergency or disaster situations;
evaluating public health programs;
drinking water and environmental management;
food, drug, and radiation safety;
terrorism preparedness;
public health services; and
public health research.

Both federal and state government agencies may receive personal health information for public health purposes. Examples of such agencies include California’s Department of Public Health, the Centers for Disease Control, the National Institutes of Health, the Food and Drug Administration, the Federal Emergency Management Administration, and the Occupational Health and Safety Administration.

You can request information about public health disclosures to see who has received your information, the dates of disclosures, a summary of what was disclosed, and a brief explanation of the reasons for disclosure or a copy of the request. To learn how to request an accounting of disclosures, see the California Department of Public Health website. [28]

h. Employers

There are many ways employers can get health and medical information, but most of the time that information won’t come directly from your health care provider or insurer without your authorization or consent. For in-depth information about how employers and prospective employers may have access to your health and medical information, see PRC’s California Medical Privacy Guide: Employment and Your Medical Privacy [29].

Note that in California, CMIA requires employers who receive your medical information to “establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information.” Cal. Civ. Code § 56.20(a) [30].

If your employer offers an employer-sponsored plan (sometimes also called self-funded plan or self-insured plan), they will receive the information other health insurers receive. The employer will also be required to comply with both CMIA and HIPAA with respect to any medical or protected health information.

Health care providers or health plans that create medical information as a result of employment-related health care services (conducted at the employer’s request and expense) may disclose information to the employer when the medical information is relevant in a lawsuit, arbitration, grievance, or other claim or challenge involving you and your employer where you place your medical history, mental or physical condition, or treatment at issue. In these situations, medical information may only be used or disclosed in connection with the proceeding. Cal. Civ. Code § 56.10(c)(8)(a) [14].

In addition, health care providers or health plans that create medical information as a result of employment-related health care services (conducted at the employer’s request and expense) may disclose information to the employer when the medical information describes functional limitations that may entitle you to take leave from work for medical reasons or limit your fitness to perform your present employment. No statement of medical cause may be included in the information disclosed to the employer. Cal. Civ. Code § 56.10(c)(8)(b) [14].

i. Insurers

Insurers cannot access your actual medical record without your authorization. But they do receive treatment codes from health care providers so they know how much to pay the provider and can determine your share of payment. While insurers do not receive your actual medical record, billing codes can provide enough information to create an outline of your medical history.

Certain insurers may obtain additional health and medical information from prescription drug and MIB reports.

**Prescription drug reports**

Insurers often purchase prescription drug reports to evaluate applications for individual life insurance or disability policies.
For more information on prescription privacy, see PRC’s California Medical Privacy Guide: Your Prescriptions and Your Privacy [31].

The Medical Information Bureau

The Medical Information Bureau (MIB) is a company that maintains a database of individual medical and other information for member insurance companies. The MIB database contains information about medical conditions and diagnostic tests, reported by insurers and based on information they receive when you apply for an MIB member insurance policy. MIB does not receive actual medical records.

MIB member companies use the database to assess risk and prevent fraud on insurance applications. MIB data is often used for underwriting life, disability, long-term care, and automobile insurance that includes medical coverage.

To find out if you are in the MIB database and to access your report (if one exists), you may request a free MIB report annually by calling 866-692-6901 or visiting the MIB website [32]. If you have never applied for insurance that required individual underwriting, or if it has been more than seven years since you applied, the MIB should not have any information on you. For more information on the MIB and your rights, see PRC’s Guide: “Other” Consumer Reports: What You Should Know About “Specialty” Reports [33].

8. Can your health information be used or disclosed outside the healthcare context without your authorization or consent?

Yes. If you disclose your information to a person or business that isn’t covered under CMIA or HIPAA, that information can be used for almost any purpose unless there is another law that applies. In addition, data breaches are quite common. For more information about various other privacy issues concerning health and medical information, see PRC’s health and medical privacy resources [34].

9. Resources

To find the full text of California laws, visit the California Legislation Information website [35].

California Department of Public Health

[36]Phone: (916) 558-1784

California Attorney General’s Office

[37]Phone: (800) 952-5225

U.S. Department of Health and Human Services [38]

Phone: (877) 696-6775

Originally funded in 2012 with cy pres award from Rodriguez et al. v. NDHealth et al.

Updated in 2017 with funding from the Rose Foundation for Communities and the Environment.


Links

[2] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=HSC&division=106.&title=&amp;part=1.&amp;chapter=1.&amp;article=