1. What does this guide cover?

This guide briefly summarizes many of the laws that apply to California residents’ health and medical information.

2. Federal health and medical privacy laws

The two primary federal laws that apply to health and medical information are the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Nondiscrimination Act (GINA).

   a. The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA requires health care providers, health plans, and health care providers (called covered entities) to comply with privacy and security rules. HIPAA provides baseline protections for health information and allows states to enact stronger laws.


   b. The Genetic Information Nondiscrimination Act (GINA)

GINA prohibits employers and health insurers from discriminating against you on the basis of genetic information. It prohibits employers and most health insurers from requesting, requiring you to provide, and purchasing genetic information in most situations. Pub. L. No. 110-233, 122 STAT. 881 (2008) [7]. GINA does not apply to employers with fewer than 15 employees. Nor does it apply to life, disability, or long-term care insurers.

   Note that California law (CalGINA [8]) is broader than GINA and also prohibits genetic discrimination in housing, mortgage lending, employment, education, and public accommodations.

   For more information about how GINA applies in the employment context, see the U.S. Equal Employment Opportunity
Commission’s resources [9]. The U.S. Department of Health and Human Services’ site contains additional information [10] about GINA in the health insurance context.

3. California health and medical privacy laws

a. Confidentiality of Medical Information Act (CMIA)


CMIA’s primary purpose is to protect an individual’s medical information, in electronic or paper format, from unauthorized disclosure. For more information, see PRC’s guide How is Your Health and Medical Information Used and Disclosed (California Medical Privacy Series) [12].

What information does CMIA cover?

CMIA applies to medical information. CMIA defines medical information as individually identifiable health information about a patient’s medical history, mental or physical condition, or treatment.

To be individually identifiable, information must include a data element that identifies a person such as a name, address, email address, telephone number, or Social Security number. Information is also individually identifiable if it can be combined with other publicly available information to reveal a person’s identity. Cal. Civ. Code § 56.05(j) [13]

Who must comply with CMIA?

CMIA applies to health care providers, health insurers, and individuals or businesses they contract with that have access to medical information (called contractors).

Note that CMIA’s definition of provider of health care is much broader than under HIPAA. For example, any business that offers software or hardware, including mobile apps, that is designed to maintain medical information is considered a provider of health care. Cal. Civ. Code § 56.06 [14].

CMIA also requires employers who receive medical information to safeguard that information, and prohibits them from disclosing medical information without employee authorization (though there are exceptions). Cal. Civ. Code §§ 56.20 – 56.245 [15].

Can you bring a lawsuit if your information is disclosed in violation of CMIA?


b. Information Practices Act (IPA)

The Information Practices Act (IPA) applies to state government agencies and limits collection, maintenance, and disclosure of personal information (including medical information). The IPA gives you the right to review your personal information in state agency records. You may also find out who has accessed the information and request that inaccurate or irrelevant information be changed. Cal. Civ. Code. §§ 1798-1798.78 [17]

c. Patient Access to Health Records Act (PAHRA)

The Patient Access to Health Records Act (PAHRA) gives you the right to see and copy your medical records (with some exceptions, such as psychotherapy notes) maintained by health care providers. You may also submit written addendums to records that you believe are inaccurate or incomplete. Cal. Health & Safety Code §§ 123100-123149.1 [18]

See the Medical Board of California website [19] for more information.

d. Insurance Information and Privacy Protection Act (IIPPA)

The Insurance Information and Privacy Protection Act (IIPPA) establishes standards for collection, use, and disclosure of information gathered in connection with insurance transactions such as applications and claims. The IIPPA also allows you to obtain the reasons for adverse underwriting decisions. Cal. Ins. Code §§ 791-791.29 [20]

e. Data breach notice
• **Businesses and state and local agencies** must notify you if your *personal information* has been (or is believed to have been) acquired by an unauthorized person. Personal information includes medical and health insurance information. [Cal. Civ. Code §§ 1798.29][21], [1798.82][22]

[22] The law applies to businesses and agencies that maintain unencrypted, computerized personal information, including medical and health insurance information. However, breaches of encrypted data must be reported if there is a reasonable belief that the encryption key was also acquired.

Data breach notices must be written in plain language and follow a specific format. Cal. Civ. Code §§ [1798.29(d)(1)][21] and [1798.82(d)(1)][22]

• **Health care providers, health plans, and health care clearinghouses (covered entities)** must comply with HIPAA’s data breach notice requirements. For more information see the [HHS website][23] and [45 CFR §§ 164.400-164.414][24].

   • **Additional breach notice requirements for clinics, health facilities, home health agencies, and hospices**

   Clinics, health facilities, home health agencies, and hospices must prevent unlawful or unauthorized access to, and use or disclosure of medical information. If your medical information is breached, they must notify you and the California Department of Public Health within 15 days of detection. [Cal. Health & Safety Code § 1280.15][25]

To learn more about data breach notifications, see PRC’s guide, *What to do When You Receive a Data Breach Notice* [26].

1. **Collection of medical information for direct marketing**

A business that wants to collect your medical information for direct marketing purposes must clearly disclose how the information will be used and must also get your written consent (which it may obtain online). [Cal. Civ. Code § 1798.91][27]

Note that this code section does not apply to fundraising activities by tax exempt charitable or religious organizations or political fundraising or communications.

2. **Shine the Light**

California’s Shine the Light law allows you to learn about how businesses sell your personal information, including certain types of health and medical information. [Cal. Civ. Code § 1798.83][28]

For more information on Shine the Light, see PRC’s guide, *California’s “Shine the Light” Marketing and Junk Mail Law* [29].

3. **Online Privacy Protection Act**

The Online Privacy Protection Act requires websites or online services that collect personally identifiable information to conspicuously post a privacy policy that identifies the data it collects and discloses with whom that data is shared. [Cal. Bus. & Prof. Code § 22575(a)][30]

For more information on the Online Privacy Protection Act, see the CA AG Office’s publications, *Making Your Privacy Practices Public* [31] and *How to Read a Privacy Policy* [32].

4. **Privacy protections for psychiatric records**

The California Welfare and Institutions Code protects the confidentiality of records of people who are voluntarily or involuntarily detained for psychiatric evaluation or treatment. [Cal. Welfare & Institutions Code § 5328][33]

5. **Privacy protections for HIV blood tests**

The California Health and Safety Code contains provisions to protect the privacy of people who are subject to HIV blood testing. [Cal. Health & Safety Code § 120975 – 121020][34]

6. **Office of Health Information Integrity**


CalOHII provides oversight and assistance to California state departments to ensure that they comply with health privacy laws.
and safeguard health information.

4. Additional Resources

To find the full text of California laws, visit California Legislative Information [37].

California Office of the Attorney General
Privacy Education and Policy Unit
[38]File a consumer complaint here [39].

For more information on California and federal health information privacy laws and regulations, see the California Health Information Law Identification (CHILI) website [40].

For more information about HIPAA, visit U.S. Department of Health and Human Services [41] or call (866) 627-7748.

World Privacy Forum
Patient's Guide to HIPAA: How to Use the Law to Guard your Health Privacy [42]

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
[15] https://www.ecfr.gov/cgi-bin/text-idx?SID=0ed84c7423abdfca1fa81d772667435a&amp;mc=true&amp;node=sp45.1.164.d&amp;rgn=div6