Michael H. Cohen Law Group, A Professional Corporation
468 North Camden Drive
Beverly Hills, California 90210
Phone: (310) 844-3173
www.michaelhcohen.com

Michael H. Cohen, JD, MBA (President)
Member of the Bar of California, Massachusetts, New York, and Washington, D.C.

WHITE PAPER -- CALIFORNIA PRIVACY & SECURITY LAWS

California privacy and security laws are extensive. Some of these legal rules apply to businesses in general, not just California healthcare providers and entities.

Whenever dealing with sensitive information—and especially when transmitting or receiving personal health information (PHI)—you should be sure to consult with an experienced California privacy and security lawyer.

This White Paper provides information about some of the most important privacy and security rules that could apply to your business.

1. Privacy

California privacy standards are contained in the Confidentiality of Medical Information Act ("CMIA").[1] Like HIPAA, these rules limit uses and disclosure of patients' personal health information.

The Health & Safety Code (sections 123100 et seq.) govern patient access to health records. (Among other things, special considerations apply to psychotherapy notes and mental health records). The California Medical Board summarizes some requirements on its webpage entitled, Patient Access to Medical Records, and Medical Records—Frequently Asked Questions.

California law also establishes a State Office of Health Information Integrity CalOHI, dedicated to informing about rights and responsibilities relevant to health information, as well as the role of electronic health information exchanges ("HIEs") in transmitting patients' health information (see Health & Safety Code, sections 130200-130205).

Among other things, CalOHI maintains the following helpful webpages:

- Preemption Analysis of State Privacy Laws
- Individual's Rights to Medical Information Privacy - FAQs
- Providers of Health Care Requirements

California's Department of Health Care Services also has a Privacy Office, which sits within the Department's Office of HIPAA Compliance, and works to protect PHI, including investigating privacy breaches and complaints involving unauthorized access or disclosure of PHI.

[1] Cal. Civ. Code ss. 56-56.37.

There is also the California Office of Privacy Protection which provides information on privacy topics for individuals and consumers. The office maintains a webpage listing privacy laws, including health information privacy. The latter page lists the following:

- Birth and Death Certificate Access - Health and Safety Code sections 103525, 103525.5, 103526, 103526.5, 103527, and 103528. Authorization is required to obtain certified copies of the birth or death certificate of another person. State and local registrars that issue non-certified copies to non-authorized applicants must print the words "informational, not a valid document to establish identity" on the copies issued.

- Birth and Death Record Indices - Health and Safety Code sections102230, 102231 and 102232. This law exempts specified compilations of birth and death records, called indices, from disclosure under the California Public Records Act. The State Registrar is required to establish separate non-comprehensive indices for public release, which do not contain Social Security numbers or mother's maiden names. Requesters of the indices must provide proof of identity and sign a form certifying, under penalty of perjury, that they will comply with prescribed usage guidelines.

- Health Facilities Data Breach - Health & Safety Code section 1280.15. This law requires certain health facilities to prevent unlawful or unauthorized access to, or use or disclosure of, a patient's medical information. It sets fines and notification requirements for breaches of patient medical information and requires facilities to report such breaches to the California Department of Public Health.

- Legal and Civil Rights of Persons Involuntarily Detained - Welfare & Institutions Code section 5328. This law provides for the confidentiality of the records of people who are voluntarily or involuntarily detained for psychiatric evaluation or treatment.

- Medical Information, Collection for Direct Marketing Purposes - Civil Code section 1798.91. This law prohibits a business from seeking to obtain medical information from an individual for direct marketing purposes without, (1) clearly disclosing how the information will be used and shared, and (2) getting the individual's consent.

- Medical Information Confidentiality - Civil Code sections 56-56.37 This law puts limits on the disclosure of patients' medical information by medical providers, health plans, pharmaceutical companies, and many businesses organized for the purpose of maintaining medical information. It specifically prohibits many types of marketing uses and disclosures. It requires an electronic health or medical record system to protect the integrity of electronic medical information and to automatically record and preserve any change or deletion.

- Mandated Blood Testing and Confidentiality to Protect Public Health - Health & Safety Code sections 120975-121020. This law protects the privacy of individuals who are the subject of blood testing for antibodies to the probable causative agent of acquired immune deficiency syndrome (AIDS).

- Office of Health Information Integrity - Health and Safety Code sections 130200-130205. This law established the Office of Health Information Integrity in the California Health and Human Services Agency, with the mission of ensuring enforcement of state law on the confidentiality of medical information.

- Patient Access to Health Records - Health & Safety Code section 123110 and following. With minor limitations, this law gives patients the right to see and copy information maintained by health care providers relating to the patients' health conditions. The law also gives patients the right to submit amendments to their records, if the patients believe that the records are inaccurate or incomplete.

The Department further has a webpage on Notice of Privacy Practices and the Health Insurance Portability and Accountability Act (HIPAA).

Penalties for violations can be substantial. For example, under California Civil Code section 56.36, any violation of the California Confidentiality of Medical Information Act that results in economic loss or personal injury to a patient is punishable as a misdemeanor. Further, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) nominal damages of $1,000 (*i.e.*, irrespective of injury); (2) the amount of actual damages suffering.

2. Security—Health Care Providers

Section 130203 provides:

> (a) Every provider of health care as defined in Civil Code sections 56.05(j) shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information. Every provider of health care as defined in Civil Code sections 56.05(j) shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use or disclosure.
>
> (b) In exercising its duties pursuant to this division, the office shall consider the provider's capability, complexity, size, and history of compliance with this section and other related state and federal statutes and regulations, the extent to which the provider detected violations and took steps to immediately correct and prevent past violations from reoccurring, and factors beyond the provider's immediate control that restricted the facility's ability to comply with this section.

3. Security—Businesses Generally

More generally, California law addresses security requirements for businesses in California Civil Code, sections 1798.80-1798.84. Requirements include:

- A business must take reasonable steps to dispose, or arrange for the disposal, of customer records containing "personal information," by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information to make it unreadable or undecipherable.[2]

- A business that "owns or licenses" personal information about a California patient must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," to protect the information from unauthorized access, destruction, use, modification, or disclosure.[3]

- A business that discloses personal information pursuant to a contract with a third party must require by contract that the party third implement and maintain reasonable security procedures and practices.[4]

There are various exceptions to the above rules, including:[5]

- A provider of health care regulated by the Confidentiality of Medical Information Act;

- A covered entity under HIPAA.

However, the statute goes on to regulate data breaches:[6]

- Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, must disclose any breach of security, following discovery, to any California patient whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

- Any person or business that maintains computerized data that includes personal information that the person or business does not own, must disclose any breach of security, following discovery, to any California patient whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

- There are specific requirements for the breach notification. A Covered Entity that complies with the HITECH breach notification requirements is deemed to have complied with California law.

    - A breach that involves more than 500 California patients requires disclosure to the Attorney General.

---

[2] Cal. Civ. Code s. 1798.81. "Personal information" means any information that "identifies, relates to, describes, or is capable of being associated with, a particularly individual," including his or her name. Id. S. 1798.80.
[3] Id., s. 1798.81.5(b). "Owns or licenses" includes retaining the information as part of the business's internal customer account."
[4] Id., s. 1798.81.5(c).
[5] Id., s. 1798.81.5(e).
[6] Id., s. 1798.82.

- There are additional requirements if disclosure was made to third parties that use the personal information for marketing purposes.[7]

- Businesses must have an online privacy policy (labeled "Your Privacy Rights").[8]

This document provides a general summary of relevant California laws. It is critical to consult an experience privacy and security attorney for legal advice concerning HIPAA as well as state law privacy and security (or cyber-security) advice.[9]

[7] Id., s. 1798.83.
[8] See id., 1798.83 for specific requirements; 1798.83(d) for exempted disclosures; and 1798.84 for penalties.
[9] These materials have been prepared by the Michael H. Cohen Law Group ("Law Firm") for informational purposes only and are not legal advice or counsel. Transmission of the information is not intended to create, and receipt does not constitute, an attorney-client relationship. Readers should not act upon any information in this website without seeking professional counsel. This is not intended to be advertising and neither the Law Firm nor any of its attorneys wish to represent anyone desiring representation based upon reading these materials in a state where this website fails to comply with all laws and ethical rules of that state.