BakerHostetler

# California

Calif. Civ. Code §§ 1798.29, 1798.81.5, 1798.82, 1798.150 (as amended, 2019), 1798.80, 1798.84; Calif. Health and Safety Code § 1280.15 (2015)

## Quick Notes

- "Personal Information" is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is not permitted in determining when notification is triggered.
- Under the general breach notification statute, notice to the Attorney General or State Agency is required in a specific format if more than 500 California residents must be notified. Under the medical information specific breach notification statute, the California Department of Health Services must be notified no later than 15 business days after the detection of a breach.
- Under the general breach notification statute, notice is not required within an explicit number of days. Under the medical information specific breach notification statute, affected individuals and the California Department of Health Services must be notified no later than 15 business days after a breach of security.
- Under the general breach notification statute, a private cause of action is permitted and the California Consumer Privacy Act (CCPA) changes permit a private cause of action for breaches under the general breach notification statute that violate the obligations of CCPA. Under the medical information specific breach notification statute, a private cause of action is not permitted.

## Personal Information Definition

Under the general breach notification statute, PI is an individual's first name or first initial and last name plus one or more of the following data elements:

1. Social Security number.
2. Driver's license number or state-issued ID card number.
3. Passport number, Tax Identification Number, Military Identification Number, or other unique identification number issued on a government document used to verify the identity of an individual.
4. Account number, credit card number or debit card number.
5. A username or email address in combination with a password or a security question and answer that would permit access to an online account.
6. Information or data collected through the use or operation of an automated license plate recognition system.
7. Medical information and health insurance information.
8. Unique biometric data generated from measurements or technical analysis of a human body characteristic.
9. Genetic data

The Medical Information Specific Breach Notification Statute protects "Medical Information" (see full text statute).

## Persons Covered

Any state agency, person or business who conducts business in California and owns, licenses or maintains computerized data that includes personal information is covered under the General Breach Notification Statute.

Clinics, health facilities, home health agencies and hospices licensed pursuant to sections 1204, 1250, 1725 or 1745 of the California Health and Safety Code are covered under the Medical Information Specific Breach Notification Statute.

## Encryption/Notification Trigger

The General Breach Notification Statute applies where the information is either (a) not encrypted or (b) encrypted, if an encryption key or security credential that allows an unauthorized party to render the data readable or usable is also compromised.

Standard for Triggering: The statute is triggered upon discovery or notification of the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the entity.

The Medical Information Specific Breach Notification Statute is triggered by any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information.

## Specific Content Requirements

Under the General Breach Notification Statute, notification to California residents must be in written form, using plain language in no smaller than 10-point type. The notification shall be titled "Notice of Data Breach" and use all of the following clearly and conspicuously displayed headings:

(1) "What Happened"

(2) "What Information Was Involved"

(3) "What We Are Doing"

(4) "What You Can Do"

(5) "For More Information"

The breach notification must include four elements: (1) the date of the notice; (2) the name and contact information of the person reporting a breach; (3) a list of the types of personal information likely impacted; and (4) if the breach exposed a Social Security number or a driver's license or CA identification card number, the toll-free telephone numbers and addresses of the major credit reporting agencies.

If the breach may have exposed Social Security numbers or driver's license or CA identification card numbers, the entity must provide appropriate identity theft protection and mitigation services at no cost to the affected persons for not less than 12 months.

If the breach only involved a username or email address in combination with a password or security question permitting access to an online account, notice to CA residents may be in electronic or other form that directs the affected individual to promptly change his or her password and security question answer or take other precautionary security steps.

If the breach involved login credentials of an email account furnished by an entity, the entity must provide notice to that email address as well as by another "clear and conspicuous" method, delivered to the resident online when the resident is connected to the online account from an IP address or online location from which the entity knows the resident customarily accesses the account.

## Timing

Under the General Breach Notification Statute, disclosure shall be made "expediently" and without "unreasonable delay," consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the integrity of the data system.

If an entity maintains computerized data that includes personal information that the entity does not own, the entity must notify the owner or licensee of the information of any breach immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Under the Medical Information Specific Breach Notification Statute, affected patients and the California Department of Health Services must be notified no later than 15 business days after the unauthorized access, use or disclosure has been detected by the licensee. This notice can be delayed for law enforcement purposes so long as the delay is documented in accordance with the requirements of section 1280.15(c) of the California Health and Safety Code.

## Penalty/Private Right of Action

Under CCPA's private right of action provision § 1798.150, nonencrypted and nonredacted personal information defined by the General Breach Notification Statute subject to unauthorized access and exfiltration due to a business's violation of the duty to implement and maintain reasonable security procedures and practices will allow for a civil action to recover damages not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater. Additionally, injunctive or declaratory relief and other relief deemed proper by the court may be granted.

Under the General Breach Notification Statute, any customer injured by a violation of § 1798.82 may institute a civil action to recover damages. Also, any business that violates or proposes to violate § 1798.82 may be enjoined.

There is a “Safe Harbor Exception” for a record custodian who properly disposes of records.

Under the Medical Information Specific Breach Notification Statute, the California Department of Health Services may impose the following penalties against licensees who violate section 1280.15:

(1) $25,000 per patient whose information was affected, and up to $17,500 per subsequent occurrence.

(2) Entities that fail to report the incident to the State Department of Health Services or the affected patients within the 15-day time period absent lawful delay are subject to a penalty of $100 per day.

(3) The total penalties imposed may not exceed $250,000 per reported event.

## Other Provisions

Under the General Breach Notification Statute, any person who notifies more than 500 California residents as a result of a single breach must complete and submit the Attorney General’s Data Security Breach form, and attach a single sample copy of the notification letter sent to the affected California residents.

Under the Medical Information Specific Breach Notification Statute, the California Department of Health Services must be notified no later than 15 business days after the unauthorized access, use or disclosure has been detected by the licensee.