

HANDLING OF PERSONAL AND/OR CONFIDENTIAL INFORMATION

0939

(No.34 January 2016)

All information classified as personal and/or confidential must be properly stored, transmitted, and disposed of in order to protect it from unauthorized access, disclosure, and/or modification.

REFERENCE(S)

0939.1

(No.34 January 2016)

Article 1, Section 1, of the Constitution of the State of California
State Administrative Manual (SAM) Sections [5300.3](#), [5310](#), and [5350.1](#)
Government Code Sections [11019.9](#) and [19572](#)
[Information Practices Act of 1977 \(Civil Code Sections 1798 et seq.\)](#)
[Confidentiality of Medical Information Act \(Civil Code Sections 56 et seq.\)](#)
[California Financial Information Privacy Act \(Financial Code Sections 4050-4060\)](#)
Health Insurance and Portability Accountability Act of 1996 (HIPAA)
[California Penal Code Section 502](#)
[CAL FIRE 0900 Information Technology Handbook, Section 0934](#)
Federal Information Processing Standards
National Institute of Standards and Technology Special Publication 800-53

GENERAL PROVISIONS

0939.2

(No.34 January 2016)

It is the responsibility of the data owner to ensure data users are aware of the proper handling techniques for the information they access. Users of data classified as personal and/or confidential, at minimum, are required to know, understand, and follow the policies established herein. Certain information may require additional levels of security. The minimum standards outlined in this policy do not absolve responsibility from data owners for compliance with any additional mandates, including, but not limited to, State and/or Federal law requirements.

DEFINITIONS

For purposes of this policy, please find the following definitions:

- Data Owner – Program management responsible for the accountability of the data, asset, or system. The data owner is primarily responsible for the business rules, asset management, and compliance with applicable mandates.
- Data User – A person who uses the data, asset, or system.

- Confidential Information – Any records (i.e., automated, electronic, video, photographic, audio, and/or paper) that have restrictions on disclosures in accordance with other applicable mandates including, but not limited to, State and/or Federal laws.
- Personal Information – Commonly referred to as personally identifiable information (PII). PII means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. PII includes statements made by, or attributed to, the individual. PII typically refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Dependent on the applicable mandate, definitions may vary. Provided below are legal excerpts to assist in gaining a general understanding of the types of protected information deemed personal and/or confidential:

- **The Information Practices Act**, Civil Code Section 1798.3(a), states in part that personal information means any information that is maintained by a department that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.
- **The Confidentiality of Medical Information Act**, Civil Code Section 56.05(j), states in part that medical information means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. Individually identifiable means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.
- **The California Financial Information Privacy Act**, Financial Code Section 4052 (b), states in part that personally identifiable financial information includes all of the following:
 - (1) Information a consumer provides to a financial institution on an application to obtain a loan, credit card, or other financial product or service.

- (2) Account balance information, payment history, overdraft history, and credit or debit card purchase information.
 - (3) The fact that an individual is or has been a consumer of a financial institution or has obtained a financial product or service from a financial institution.
 - (4) Any information about a financial institution's consumer if it is disclosed in a manner that indicates that the individual is or has been the financial institution's consumer.
 - (5) Any information that a consumer provides to a financial institution or that a financial institution or its agent otherwise obtains in connection with collecting on a loan or servicing a loan.
 - (6) Any personally identifiable financial information collected through an Internet cookie or an information collecting device from a Web server.
 - (7) Information from a consumer report.
- **The [HIPAA Privacy Rule](#)** protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The HIPAA Privacy Rule calls this information protected health information (PHI).

Individually identifiable health information is information, including demographic data, that relates to: 1) the individual's past, present, or future physical or mental health or condition, 2) the provision of health care to the individual, or 3) the past, present, or future payment for the provision of health care to the individual, and 4) that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number).

These mandates place very specific restrictions, among other requirements, on the collection, use, dissemination, and maintenance of protected information. It is important that all data owners and data users accessing such information are aware of the various restrictions required for compliance.

STORAGE

All data classified as personal and/or confidential shall be stored in a secure manner.

Data owners should clearly define where the personal and/or confidential information can be stored and have the storage resources available for the data users.

- **Electronic data** classified as personal and/or confidential shall be stored within the network environment with limited exceptions. To ensure proper backup and recovery of personal and/or confidential information is performed, the storage of such data on devices (e.g. hard drives) is prohibited unless an exception is approved by the CAL FIRE Chief Information Officer (CIO) and the CAL FIRE Information Security Officer (ISO).
 - Permission from the data owner, with limited exceptions, is required prior to storing any personal and/or confidential information on portable electronic storage media or personal telecommunications devices. If permission is granted, the device(s) must be encrypted. (See [CAL FIRE 0900 Information Technology Services Handbook](#).)
 - Multifunction Printers (MFPs) must be securely configured. (See SAM and NIST.)
- **Paper data** classified as personal and/or confidential shall be stored securely within a locked environment (e.g., lock and key, keypad, access card control). (See [CAL FIRE 2100 Paperwork Management Handbook](#).)

All personal and/or confidential information requiring access will be controlled using role-based authorizations and maintained by the data owner for audit purposes. Furthermore, applicable mandates may require additional, specific safeguards employed for the purposes of storing protected electronic and/or paper data. For example, the [HIPAA Security Rule](#) sets national standards for the security of electronic PHI. Refer to the respective statute(s) for additional information.

TRANSMISSION

All data classified as personal and/or confidential shall be transmitted in a secure manner.

- **Transmission of electronic data classified as personal and/or confidential shall be redacted or encrypted.** Generally, personal information should never be used on email. If protected data must be transmitted, either in the body of an email or as an attachment, the email must be encrypted. Prior to sending an email, the employee must ensure the email is being sent to the proper email address.

If an email containing personal and/or confidential information is sent or received by any employee and it is not encrypted, the employee must report it to the ISO immediately. (See [CAL FIRE 0900 Information Technology Services Handbook, Section 0938](#).)

- Transmission of **paper data** classified as personal and/or confidential shall be secured as much as possible recognizing that the transit of materials is often-times beyond user control. Consider the following safeguards:
 - Redact, if possible.
 - Hand-deliver, if possible.
 - When shipping documents:
 - Package in such a way that personal and/or confidential information is not viewable.
 - Inspect destination addresses thoroughly.
 - Ensure correct return address is provided.
 - Review contents to verify that only appropriate information for the intended recipient is packaged.
 - Secure packages.
 - If possible, use shipment tracking and/or confirmation of delivery methods of shipment.

Applicable mandates may specify additional transmission requirements as well as access requirements including, but not limited to, who can receive the data, how data can be received, and what types of data can be shared. System agreements (e.g., the State Controller's Office system, the Department of Justice system) may further define requirements of usage.

Any restrictions established that are more stringent than those within this policy should be documented in procedures and clearly communicated to all data users.

DISPOSAL

All personal and/or confidential information must be properly sanitized prior to disposal in accordance with approved record retention schedules. It is the responsibility of the data owner to ensure that all record retention requirements are fulfilled prior to the disposal of the information.

Data owners should work with the Information Technology Services Coordinator and/or the Business Services Office Records Management Coordinator to determine the disposal method options available based on current sanitization methods used and supported by the Department.

- **Electronic data** classified as personal and/or confidential shall be sanitized in accordance with Departmental policy. (See [CAL FIRE 0900 Information Technology Services, Section 0925.](#))
 - This also applies to hard drives in MFPs regardless of the type of information copied, printed, faxed, scanned, or stored.

- **Paper data** classified as personal and/or confidential shall be disposed of in accordance with Departmental policy. (See [CAL FIRE 2100 Paperwork Management Handbook Section 2170 et seq.](#))

MISHANDLING

Personal and/or confidential information must be handled in such a manner that it does not become misplaced or available to unauthorized personnel. Personal and/or confidential information shall only be disclosed to employees where the information is relevant and necessary to their duties. The data owner must ensure that authorizations are documented and maintained.

Any mishandling of personal and/or confidential information while stored, transmitted, or disposed of resulting in suspected or actual unauthorized access, disclosure, and/or modification must be reported to the ISO in accordance with the [CAL FIRE 0900 Information Technology Services Handbook Section 0938](#).

Furthermore, any unauthorized use or disclosure of personal and/or confidential information may result in civil or criminal penalties, as well as disciplinary action under Government Code Section 19572, Civil Code Section 1798.55, and/or California Penal Code Section 502.

[\(see next section\)](#)

[\(see HB Table of Contents\)](#)