START

Data Encrypted? (min. 128-bit)

Encryption key compromised or data accessed?

No

Medical Information?

(1)

No

Electronic Information?

Yes

Personal Information?

(5)

No

System Security Breach?

(6)

Yes

California Resident?


NOTIFICATION REQUIRED

[California Civil Code 1798.29]

Notification to California residents must occur in the most expedient time possible and without unreasonable delay, except when a law enforcement agency has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation) or when necessary to discover the scope of the breach and restore the integrity of the system.

If the University is maintaining personal information owned by another agency and that information is breached, the owner agency must be notified immediately.

In coordination with Campus Counsel, notice must be made in written, hard-copy form or via e-mail. Telephone communication or other timely communication to an individual’s representative may be used when it is determined that written notice may adversely affect a patient’s health.

If sufficient contact information is not available for direct hard-copy or e-mail notice, a substitute method of notice may be used. Substitute notice shall include prominent display on the campus’s Web site or other commonly used Web site for at least forty-five days. Both Campus Counsel and the campus community relations or public information office should be consulted to develop the substitute notice.

NOTIFICATION REQUIRED WITHIN 5 BUSINESS DAYS

[California Health and Safety Code 1280.15]

Written notice must be provided to CDPH and the affected patient (or his or her representative) within five business days after the unlawful or unauthorized access, use or disclosure has been detected. Facilities should not wait until they have conducted a preliminary review to report a breach. Misdirected internal paper records, email, or fax transmissions to another health care worker within the same facility or health care system for the purpose of coordinating care or delivery of services do not need to be reported.

CDPH has advised that notification should be sent to the patient’s (or patient representative’s) last known address.

When notifying CDPH, the following information should be included:
- date and time of reported incident
- facility name
- facility address
- facility contact person
- name of patient(s)
- name of alleged violators
- general information about the circumstances of the breach
- any other information needed to make the determination for an onsite investigation

Decisions to notify or not notify should be well documented.

See next page for numbered “(n)” definitions.

For updates, please contact Russell Opland
Systemwide Privacy Officer, University of California
Russell.Opland@ucop.edu
Definitions:

(1) “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.

(2) “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.

(3) “Licensed Facility”: California Department of Public Health (CDPH) licensed facilities include those hospitals, hospices, clinics, home health agencies and hospices licensed by CDPH.

- Unlicensed, freestanding clinics owned and operated by UC are **not** licensed facilities for purposes of this analysis.

(4) “Unauthorized Access” means the inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by the California Medical Information Act (CMIA), HIPAA or other statute or regulation governing medical information.

- The University should **NOT** report misdirected records, emails or faxes to another University employee within UC for the purposes of coordination of care or delivery of services.

(5) “Personal Information” is defined as an individual’s first name or first initial, and last name, in combination with any one or more of the following:

- social security number
- driver’s license number or California Identification card number
- financial account number, credit card number or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account
- medical information (any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional)
- health insurance information (an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including appeals records)

(6) “System security breach” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.