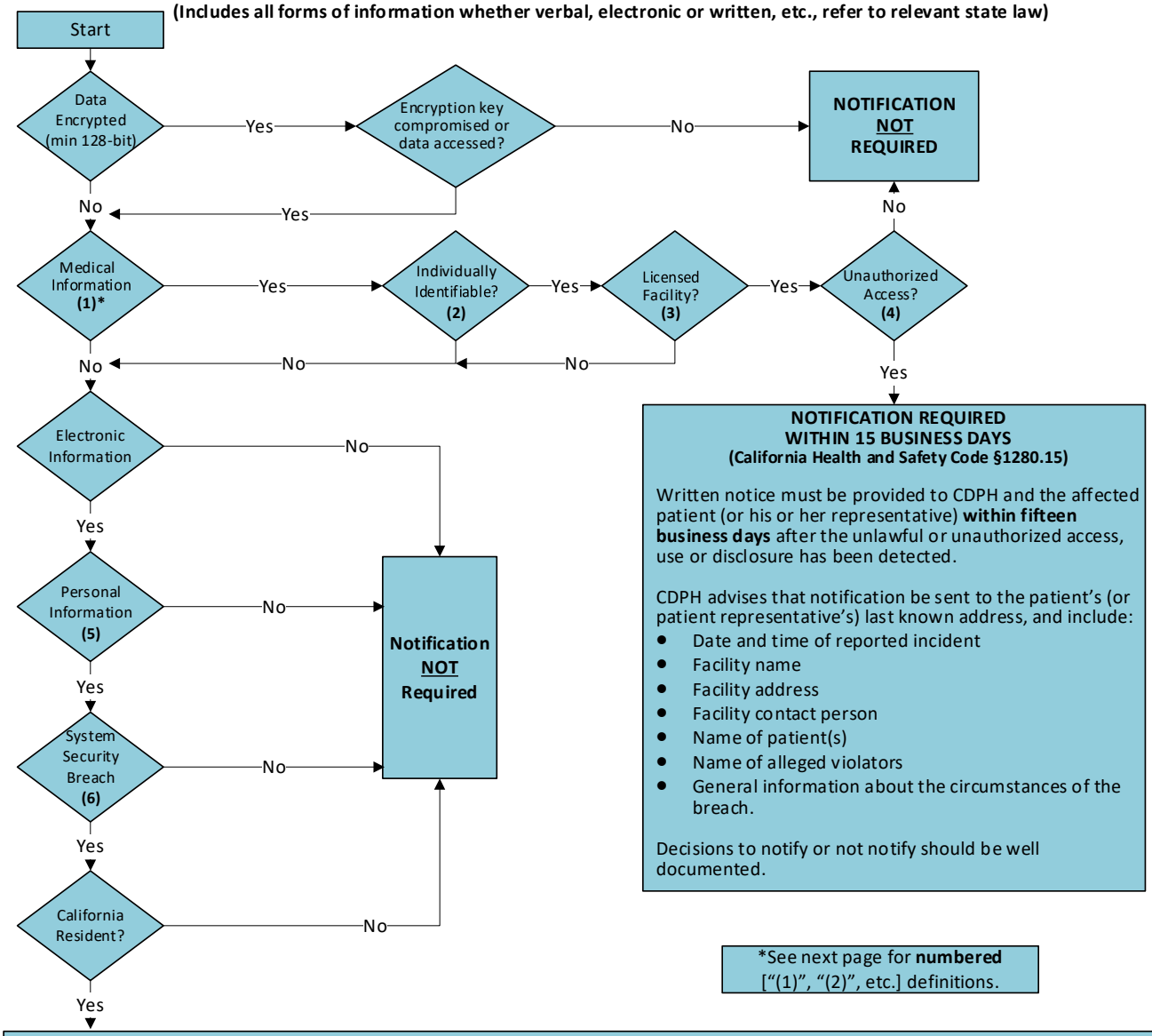
University of California Information Breach Decision Tree for California State Law

(Includes all forms of information whether verbal, electronic or written, etc., refer to relevant state law)



NOTIFICATION REQUIRED
WITHIN 15 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 fifteen business days** after the unlawful or unauthorized access, use or disclosure has been detected.

CDPH advises that notification be sent to the patient's (or patient representative's) last known address, and include:

- 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.

Decisions to notify or not notify should be well documented.

*See next page for **numbered** ["(1)", "(2)", etc.] definitions.

NOTIFICATION REQUIRED
(California Civil Code §1798.29)
https://oag.ca.gov/privacy/databreach/reporting

The individual must be notified in writing "in the most expedient time possible and without unreasonable delay". If the University is maintaining personal information owned by another agency and that information is breached, the owner agency must be immediately notified.

Notice **must** be made:

- In plain language **AND**
- In writing; **or** electronic notice if the individual has consented to receive communications by electronic means; **or** substitute notice, if the University demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the University does not have sufficient contact information. Substitute notice shall consist of all of the following:
  - i. E-mail notice when the University has an email address for the subject persons
  - ii. Conspicuous posting of the notice on the University's web site
  - iii. Notification to major statewide media.

Notice **must** include:

- The name and contact information of the facility
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach
- Date of the notice
- Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number, and
- If determinable at the time the notice is provided, any of the following:
  - i. the date of the breach,
  - ii. the estimated date of the breach, or
  - iii. the date range within which the breach occurred.

If the breach involved >500 California residents, University must submit a sample copy of the notification electronically to the CA Attorney General. If University notified the Office of Civil Rights pursuant to the HIPAA breach notification rule, University need not notify individuals under the IPA. Notification to the CA Attorney General is still required if the breach involved >500 CA residents.

UCOP ECAS February 2020

University of California Information Breach Decision Tree for California State Law
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.
    a. 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.
    a. 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
    a. First name or first initial, and last name, in combination with any of the following:
        i. Social security number;
        ii. Driver's license number
        iii. California identification card number;
        iv. Other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
        v. Medical information, defined as an individual's
            1. Medical history; or
            2. Mental or physical condition; or
            3. Diagnosis by a healthcare professional.
        vi. Health insurance information, defined as an individual's
            1. Health insurance policy number or subscriber identification number; or
            2. Any unique identifier used by a health insurer to identify the individual; or
            3. Any information in an individual's application and claims history, including appeals records.
        vii. Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
        viii. Information or data collected through an automatic license plate recognition system;
    b. A username or email address, in combination with a password or security question and answer that would permit access to an online account.
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.

Note: If the information compromised is PHI held by the SHCC, the notification provisions of HIPAA/HITECH need to be considered as well.