FEDERAL AND STATE BREACH NOTIFICATION LAWS FOR CALIFORNIA

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
LEGAL CITATION	California Civil Code Section 1798.82	California Health and Safety (H&S) Code Section 1280.15	42 U.S.C. Section 17932; 45 C.F.R. Section 164.400 *et seq*.
EFFECTIVE DATE	Jan. 1, 2003	Breaches that occur on or after Jan. 1, 2009.	Breaches that occur on or after Sept. 23, 2009.
WHO MUST COMPLY	Any person or business that conducts business in California.	Health facilities licensed by the California Department of Public Health (CDPH) under H&S 1250 (hospitals, skilled-nursing facilities, psychiatric health facilities, etc.), clinics licensed under H&S 1204, home health agencies licensed under H&S 1725, and hospices licensed under H&S 1745.	Covered entities (includes hospitals, physicians, clinics, other health care professionals) that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose **"unsecured"** protected health information (PHI), their business associates and subcontractors of the business associates. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services (DHHS) in guidance. The guidance can be found at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
INFORMATION COVERED	Unencrypted computerized data containing an individual's first name or first initial and last name in combination with: 1. Social Security Number (SSN); 2. Driver's license number or California identification card number; 3. Account number, credit 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; 4. Medical information; or 5. Health insurance information, including 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 any appeals records.	A patient's **"medical information"** — 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, e-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. A breach under HIPAA or a breach of unencrypted computerized data must also be reported under this law.	PHI — individually-identifiable health information that is transmitted or maintained in electronic media or any other form or media. Individually-identifiable health information is health information (including demographic information) that identifies or can be used to identify the individual. **"Health information"** includes any information, oral or recorded in any form or medium, relating to the physical or mental health or condition of an individual, the health care provided, or payment for health care provided.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
BREACH DEFINITION	An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.	An unlawful or unauthorized access to, or use or disclosure of, a patient's medical information. **"Unauthorized"** means the inappropriate access, review, or viewing of medical information without a direct need for medical diagnosis, treatment or other lawful purpose under any state or federal law.	The acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI. Notification obligations apply if the incident involves "unsecured" PHI, which is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services (DHHS) in guidance. The guidance can be found at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
EXCEPTIONS	Good faith acquisition of personal information by an employee or agent for business purposes is not a breach if no further use/disclosure.	Internal paper records, e-mail, or faxes inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services do not constitute a breach and should not be reported.	Breach does not include: 1. Unintentional acquisition, access, or use of PHI by authorized person if made in good faith within scope of authority and no further use/disclosure in a manner not permitted by Privacy Rule. 2. Inadvertent disclosure by authorized person to another authorized person at same covered entity (CE) or business associate (BA) or organized health care arrangement, and no further use/disclosure in a manner not permitted by Privacy Rule. 3. Disclosure where CE or BA has good faith belief that the recipient would not reasonably have been able to retain the information. An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is a reportable breach, unless the covered entity demonstrates a low probability that the PHI has been compromised based on a risk assessment of the following four factors, plus any other relevant factors: 1. The nature/extent of the PHI involved, including types of identifiers and the likelihood of re-identification. 2. The unauthorized person who used the PHI or to whom the disclosure was made. 3. Whether the PHI was actually acquired or viewed. 4. The extent to which the risk to the PHI was mitigated.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
WHO MUST BE NOTIFIED	California residents (patients who live in California) State Attorney General (AG) must be sent a sample notice if more than 500 California residents were required to be notified. (Redact personally-identifiable information in sample notice sent to AG.) *See oag.ca.gov/ecrime/databreach/report-a-breach.*	Patient and CDPH	Patient, DHHS, and media if more than 500 residents of a state or jurisdiction affected. (Note that if a report is required under this law, it is virtually certain that a report must be made to CDPH under H&S 1280.15 — *see column to the left*.) For breaches by a business associate or a subcontractor of a business associate, the subcontractor must notify the business associate, and the business associate must notify the covered entity of any breach. Once the covered entity is aware of the breach, it must report the breach as explained above. The covered entity is permitted, however, to coordinate with its business associate as to who will make the notification to patients. As a result, the business associate may make the patient notification, as agreed upon by the covered entity.
TIME FRAME FOR NOTIFICATION	Notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	No later than 5 business days after detection. Must delay report upon law enforcement request.	To the patient: Without unreasonable delay and in no case later than 60 calendar days after discovery. To DHHS: Notify at the same time patients are notified, if more than 500 patients affected. Smaller breaches must be submitted via annual log each March 1 (Feb. 29 in leap years). To media: Without unreasonable delay and in no case later than 60 calendar days after discovery. Must delay notification upon law enforcement request.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
METHOD OF NOTICE	Notice may be provided by: 1. Written notice (on paper); 2. Electronic notice in conformity with the federal E-SIGN Act; or 3. Substitute notice if the costs of providing notice will exceed $250,000 or if more than 500,000 consumers are affected, or if the business does not have sufficient contact information. Substitute notice consists of: ▪ E-mail notice when the business has an e-mail address; ▪ Conspicuous posting on the website; and ▪ Notification to major statewide news media and the California Office of Privacy Protection. (The California Office of Privacy Protection no longer exists due to state budget cuts. However, the law has not been revised to delete this requirement.) However, may use another procedure in accordance with policy.	Patient must be notified "at the last known address" — this implies that notification must be done by written letter.	To the patient: Written notice or substitute notice. May notify by phone if urgent, but also need written notice. Substitute notice applies where there is insufficient or out-of-date contact information for affected patient(s). If fewer than 10 patients in this category, use alternative form of written notice, phone, or other means. If more than 10, website or media notice for 90 days. Must include toll-free phone number for 90 days. To DHHS Office for Civil Rights: Via website www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html. To media: Press release to prominent media outlets serving the state or jurisdiction where affected patients reside.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
CONTENT OF NOTICE	Must be written in plain language and include: 1. Hospital's name and contact information. 2. The types of information that were or are reasonably believed to have been released. 3. If known when the notice is provided: (a) the date of the breach, (b) the estimated date of the breach, or (c) the date range within which the breach occurred. 4. The date of the notice. 5. Whether 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. 6. A general description of the breach incident, if that information is possible to determine at the time the notice is provided. 7. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a SSN or driver's license or California ID number. However, a covered entity as defined by HIPAA is deemed to have complied with these content requirements if it has complied completely with the HIPAA content requirements *(see far right column)*.	Not specified by law. CDPH has listed elements that facilities "should" report, but the law does not require this. The elements CDPH would like in the initial report include: date and time of reported incident, facility name, facility address/location, facility contact person, name of patient(s), name of alleged violator(s), general circumstances surrounding the breach, and any other information needed to make the determination for an on site investigation. Hospitals are urged to use caution if including patient information or name of alleged violator(s) in the initial report.	To patient/media: 1. Brief description of what happened, including the date of breach and date of discovery of breach, if known. 2. Description of types of unsecured PHI involved (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, etc.). 3. Steps patients should take to protect themselves from potential harm. 4. Brief description of what CE is doing to investigate, mitigate, and protect against further breaches. 5. Contact information for patients to obtain further information, including toll-free phone number, e-mail address, website address, or street address. 6. Use plain language — translate as required under other applicable laws. To DHHS Office for Civil Rights: *See website (page 5 of this chart)*.

	BREACH OF UNENCRYPTED COMPUTERIZED DATA	BREACH IN A LICENSED HEALTH FACILITY	HIPAA BREACH REQUIREMENT
OTHER		Note that HIPAA permits "incidental disclosures" — not a breach *(see column to the right) (see also Civil Code Section 56.10(c)(14))*.	The HIPAA Privacy Rule permits an **"incidental disclosure,"** defined as: a use/disclosure "incident to" an otherwise permissible use/disclosure that occurs despite reasonable safeguards and proper minimum necessary procedures. *(See 45 C.F.R. Section 164.502(a)(1)(iii).)*