	SB 541(2007-2008)	SB 1386 (2001-2002)	HIPPA
Applicable to	Health facilities, clinics, home health agencies and hospices	All California Business owners	Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity.
Bill Provisions	Prevent unlawful or unauthorized access to, and use or disclosure of patients' medical information. "Unauthorized" 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 Confidentiality of Medical Information Act or any other statute or regulation governing the lawful access, use or disclosure of medical information.	Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in security to any California resident. "Breach of security system" is defined as unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. "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 data elements, when either the name or the data elements are not encrypted: Social security #, Driver's license #, CA ID card #, Account #, credit or debit # in combination with any required security code, access code, or password that would permit access to an individual's financial account.	Providers who maintain or transmit health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentialty of the information; protect against any reasonably anticipated threats or hazards to the security or integrity of the information and otherwise ensure compliance by their officers and employees. "health information" means any information, whether oral or recorded in any form or medium that is created or received by a provider and relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. *NOTE: For a complete list of provisions refer to the Health Insurance Portability and Accountability Act of 1996 summary at http://www.hhs.gov/ocr/privacysummary.pdf*

	SB 541 (2007-2008)	SB 1386 (2001-2002)	HIPPA
Notification Requirements	Report to Department and patient or patient representative at last known address no later than five days after the unlawful or unauthorized access, use or disclosure has been detected by the agency or hospice.	Disclose to any resident in California whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. "Notice" may be provided by one of the following methods: written or electronic. Substitute notice allowed if agency demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subjects exceeds 500,000. Substitute notice consists of: e-mail notice, conspicuous posting of notice on agency's web site page, notify major statewide media, or the agency's own information security policy procedures if they are consistent with timing requirements of the bill.	A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

	SB 541 (2007-2008)	SB 1386 (2001-2002)	HIPPA
Penalties	Up to $25,000 per patient whose medical information was unlawfully or without authorization accessed, used or disclosed up to $17,500 per subsequent occurrences of unauthorized access, use or disclosure Plus, $100 per day for not notifying the Department or patient/patient representative following the initial five days not to exceed $250,000 per reported event. Department may refer violations to Health Information Integrity for enforcement In lieu of disputing a determination, transmit to Department 75 percent of total amount of penalty for each violation within 30 business days of receipt of penalty	Any individual injured by a violation of this bill may institute a civil action to recover damages and any business that violates, proposes to violate, or has violated under this bill may be enjoined. Rights and remedies available under this bill are cumulative to each other and to any other rights and remedies available under law.	General Penalty for Neglect: $100 for each violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000. Wrongful Disclosure: A person who knowingly and in violation uses or causes to be used a unique health identifier; obtain individually identifiable health information relating to an individual or discloses individually identifiable health information to another person, shall be punished by a fine of not more than $50,000, imprisoned not more than 1 year, or both; If the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years or both.
Disputing Violation	May within ten days of receipt of penalty assessment, request a hearing. Penalties shall be paid when appeals have been exhausted and penalty upheld.	N/A	A penalty may not be imposed if the failure to comply was due to reasonable cause and not to willful neglect and the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.