

PRIVACY LAWS			UCSF - DEPARTMENT OF FAMILY AND COMMUNITY MEDICINE			Updated & Distributed 7/2/09
FEDERAL	STATE	Effective Dates	Definition	KEY REQUIREMENTS	Fines & Penalties; Civil/Criminal Actions	UC REQUIREMENTS FOR SAFEGUARDING PRIVATE INFORMATION
FERPA		8/24/1974	Federal law that protects the privacy of students' education records.	None	n/a	<ul style="list-style-type: none"> • UCSF leadership is committed to ensuring the security of protected health information (PHI) and other sensitive data. • Physically secure your work area and information when unattended: Lock up files and folders, log off your computer when away, lock the doors and windows when leaving for the day, etc. • Properly use portable devices: Store information on a department's server or other secure back-up media. Sensitive data should not be stored on portable devices • Back up your data: Backup data to a department's server, DVD, external hard drive, etc., and protect the back ups. • Use cryptic/strong passwords: Create strong passwords that are hard to guess but easy for you to remember. • Install antivirus, firewall, spyware removal, and encryption of restricted information and security updates: Ensure that every computing device is protected. • Practice safe emailing: Use UCSF secure email services whenever communicating restricted information outside of the UCSF network. • Incident Reporting Process: Report to your immediate supervisor / computer support coordinator all incidents of computer theft, loss, unusual activity, unauthorized / unfamiliar computer access, etc.
HIPAA		4/21/2005	Federal law designed to provide privacy standards to protect patients' medical records and other health information (PHI) provided to health plans, doctors, hospitals and other health care providers. Protected Health Information (PHI): any of the following data associated with health/medical information – names, dates, postal addresses, phone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan numbers, account numbers, license/certificate numbers, vehicle ID numbers, device identifiers, web URLs, IP addresses, biometric identifiers, photo/comparable images.	<p>Requires that all protected health information (PHI) have adequate security protections.</p> <p>Maintain documentation of risk assessment, monitoring and other security parameters for PHI stored electronically.</p>	<p>Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5).</p> <p>Violation of the administrative simplification regulation can result civil monetary penalties of \$100 per violation, up to \$25,000 per year.</p>	
eDiscovery		12/1/2006	Refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.	None	n/a	
SB 1386	7/1/2003	Mandates public disclosure of computer security breaches in which confidential unencrypted personal information of any California resident that may have been vulnerable. Confidential and Personal Data: Any of the following identifiers in combination with an individual's first name and last name – Academic evaluations, letters of recommendations, physical condition, psychological condition, performance evaluations, personnel corrective actions, current rate of pay, social security number, home address, home telephone number, income tax withholding financial account number, credit or debit card number and spouse or other relatives names.	<p>Requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation.</p> <p>Requires a business, as defined, to take all reasonable steps to destroy a customer's records that contain personal information when the business will no longer retain those records.</p>	The law does not impose fines or minimum prison sentences, but it does specifically allow civil lawsuits: "Any customer injured by a violation of this act may institute a civil action to recover damages."		
AB 211	1/1/2009	It prohibits a health care provider, health care service plan, or contractor from disclosing medical information regarding a patient of the provider or an enrollee or subscriber of the health care service plan without authorization. Medical Information: Medical Information is defined as information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. Health Insurance Information: Health Insurance Information is defined as 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 any appeals records.	<p>Requires health care providers to prevent unlawful access, use, or disclosure of patients' medical information</p> <p>Holds health care providers and individuals accountable for ensuring the privacy of patients' medical information</p> <p>Requires every provider of health care to implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information and to safeguard patient medical information from unauthorized or unlawful access, use, or disclosure</p>	<p>Fines and Civil penalties against any individual that negligently discloses or knowingly and willfully obtains, discloses, or uses medical information in violation of state / federal laws</p> <p>\$2,500 - \$25,000 per violation, up to \$250,000 - Maximum penalty per violation</p> <p>Misdemeanor if patient suffers economic loss or personal injury</p> <p>Potential for civil action by patient with statutory damages (\$1000) in addition to actual damages Cal-OHI may notify licensing board for further investigation/discipline of individual providers</p>		
SB 541	1/1/2009	SB 541, a companion bill, applies the AB 211 standards to licensed health facilities.	<p>Requires a licensed clinic, health facility (hospital, nursing facility or other), home health agency, or hospice to prevent unlawful or unauthorized access to, use of, or disclosure of a patient's medical information</p> <p>MUST REPORT incidents of unlawful access, use of, or disclosure of a patient's medical information WITHIN 5 DAYS of detection of the breach to the California Department of Public Health (CDPH) and the affected patient(s) / legal representative.</p>	<p>Fines to the institution of failure to prevent or report for unauthorized access, use, disclosure of medical information</p> <ul style="list-style-type: none"> • \$25,000 – Initial violation (per patient) • \$17,500 – Subsequent occurrence • \$250,000 – Maximum penalty • \$100 per day for late reporting 		