



University of California
San Francisco

December 3, 2008

ALERT

TO: All UCSF Faculty, Staff, House Staff, Students, Volunteers and Contractors

FR: Privacy Office

RE: New California Medical Privacy Laws Create a Personal Liability of up to \$250,000 per Violation

In response to recent privacy violations in California involving medical records, the Governor signed two new laws to protect patient privacy, AB 211 and SB 541, effective January 1, 2009. These two laws work together in making health care providers, that is, both hospitals and individual health care professionals, as well as University staff – accountable for maintaining the confidentiality of patient medical information. Individuals will face fines and penalties, for which they will be personally responsible, criminal sanctions, as well as disciplinary action by licensing boards for unauthorized access/disclosure of medical information. In addition, hospitals will incur fines for failure to prevent or report unauthorized access/disclosure of medical information. The attached chart highlights each law.

The new laws define unauthorized access as:

“The inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the California Medical Information Act.”

Both the University of California and UCSF have existing privacy policies that are consistent with these new laws. Current privacy policies provide that unauthorized access, use, disclosure and viewing of medical information are unlawful and subject to sanctions and disciplinary actions up to and including termination of employment.

If you access Protected Health Information (PHI) or Personally Identifiable Information (PII), you are personally responsible for ensuring the confidentiality, privacy, and security of the data entrusted to you, and you could be personally subject to statutory fines and penalties for failure to comply. You are expected to:

- Access, use, disclose only the minimum necessary amount of information
- Use safeguards to protect verbal, written, electronic health information including encryption software
- The “Secure” e-mail system must be used if ePHI is in the e-mail message
- Dispose of health information appropriately De-identify information whenever possible
- Protect your password(s), do not share passwords, log off promptly and use computing device security

It is critical that you report incidents immediately (due to the new 5 day reporting requirement). Report suspected privacy violations to the UCSF Privacy Office. Report lost or stolen computers promptly to the UCSF Police (415-476-1414), and if PHI is involved, call the UCSF Privacy Office (415-353-2750) as well:

Going forward, UCSF will enhance encryption activities on the campus; enhance controls on clinical systems; and implement more robust monitoring and surveillance of electronic records to detect for unauthorized access.

For questions concerning privacy or data security, call any of the following:

- UCSF Chief Privacy Officer: 415-353-2750
- UCSF Medical Center, Information Security Officer: 415-353-3539
- UCSF Information Security Officer: 415-502-1593

Highlights of the New Medical Privacy Laws Effective January 1, 2009

	AB 211	SB 541
Key Requirements	Mandates the confidentiality of medical information. Requires implementation of appropriate administrative, technical and physical safeguards to protect the privacy of a patient's medical information, and implementation of reasonable safeguards to prevent unauthorized access, use, or disclosure.	Mandates prevention of unlawful or unauthorized access to or use or disclosure of patient medical information. Reporting obligations: Providers must report incidents of unlawful access, use, or disclosure of a patient's medical information within 5 days of detection of the breach to CDPH and the affected patient(s)/ legal representative.
Authorizes	Fines and civil penalties <u>against any individual</u> that negligently discloses or knowingly and willfully obtains, discloses, or uses medical information in violation of state / federal laws.	Fines to the institution for failure to prevent or report for unauthorized access, use, disclosure of medical information.
Oversight Agency	Calif. Office of Health Information Integrity (Cal-OHII)	Calif. Department of Public Health (CDPH)
Fines & Penalties; Civil/Criminal Actions	<u>Individual Fines/ Penalties:</u> \$2,500 - \$25,000 per violation \$250,000 – maximum penalty per violation Misdemeanor if patient suffers economic loss or personal injury 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.	<u>Institutional Fines for failure to prevent or report:</u> \$25,000 – initial violation (per patient) \$17,500 – subsequent occurrence \$250,000 – maximum penalty \$100 per day for late reporting

Refer to the State's web-sites to review the new privacy laws:

AB-211: http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0201-0250/ab_211_bill_20080930_chaptered.pdf

SB-541: http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0501-0550/sb_541_bill_20080930_chaptered.pdf