From: Internal Communications
Subject: NEW STATE PRIVACY LAWS -- Personal Liability Up to $250,000 Per Violation
Date: Tuesday, December 16, 2008 1:41:34 PM
Attachments: Medical_Privacy_chart.rtf

TO: UCSF EMPLOYEES, STUDENTS, VOLUNTEERS AND CONTRACTORS

FROM: Deborah Yano-Fong, RN, MSN, CHP
Chief Privacy Officer
deborah.fong@ucsfmedctr.org

RE: NEW STATE MEDICAL PRIVACY LAWS
PERSONAL LIABILITY 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 Jan. 1. These two laws work together to make 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 and disciplinary action by licensing boards for unauthorized access or disclosure of medical information. In addition, hospitals will incur fines for failure to prevent or report unauthorized access or 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 and disclose only the minimum necessary amount of information.
- § Use safeguards to protect verbal, written and electronic health information including encryption software.
- § The "Secure" email system must be used if ePHI is in the email message
- § Dispose of health information appropriately. "De-identify" information whenever possible.
- § Protect your passwords. Do not share passwords. Log off promptly and use computing device security.

It is critical that you report incidents immediately due to the new five-day reporting requirement.

Report suspected privacy violations to the UCSF Privacy Office. Report lost or stolen computers promptly to the UCSF Police at 476-1414. If PHI is involved, call the UCSF Privacy Office at 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.

If you have questions concerning privacy or data security, call the following:

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

For more information, see the UCSF HIPAA Web site at http://hipaa.ucsf.edu/news/default.html

Please print and distribute to our employees who don't have access to email. Thanks.