

UCSF Privacy Office

# Privacy and Confidentiality Update

Privacy Office  
2200 Post Street, C-509  
San Francisco, CA 94115-1922

Ph: 415.353.2750  
Fax: 415.353.9241  
Website: <http://hipaa.ucsf.edu/>

## New State Privacy Laws Impact Individuals, Health Care Facilities and Health Plans

“Repeated violations of patient confidentiality are potentially harmful to Californians, which is why financial penalties are needed to ensure individuals and facilities do not breach confidential medical information. Californians seeking care at a hospital or health facility should never have to worry that their private medical information will be shared.” (*Governor Arnold Schwarzenegger 09/30/08; <http://gov.ca.gov/index.php?/press-release/10693/>*)

In response to recent privacy violations in California involving medical records, the Governor signed two new laws, AB211 and SB541, which will become effective on January 1, 2009 to protect patient privacy. These laws establish a new state agency for oversight and increase state enforcement actions against health facilities as well as individuals involved in unauthorized access/disclosure of medical information. Both 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 (CMIA).”*

AB-211 legislation applies to individuals and creates the Office of Health Information Integrity (OHII) to assess fines and civil penalties (\$2,500 – \$25,000 per violation, maximum of \$250,000) against any person (licensed or unlicensed) as well as to report confidentiality violations to the appropriate licensing board for oversight, such as Medical Board, Nursing Board etc.

SB-541 applies to institutions which must have appropriate safeguards to prevent unauthorized access, use, disclosure or viewing of medical information. Incidents must be reported to both the patient and the California Department of Health (CDPH) within 5 days of detection. The CDPH can impose institutional fines of \$25,000 – \$250,000 with additional fines of \$17,500 for each

*Cont'd to pg. 2*

### Inside this issue:

New State Privacy Laws Impact Individuals Health Care and Facilities and	1-2
New Federal FTC Red Flag Rule on Medical Identity Theft	1
OCR Guidance Documents	2
Important Reminders	2
Privacy Office Web Site	2

## New Federal FTC Red Flag Rule on Medical Identity Theft

UCSF will be required to implement the Federal Trade Commission’s “Red Flags” medical identity theft prevention program which applies to any institution which extends credit. This legislation is intended to promote awareness of relevant red flags and to resolve identity theft incidents.

As the enforcement grace period has been extended until May 2009, UCSF will be providing guidance to those units affected by this new law.

There will be policy, procedures, and education

as well as a triage process for those departments or programs which extend credit, as they will be required to implement an identity theft prevention program. Red flags include:

- Inconsistencies: medical history vs. treatment (height, allergies)
- Suspicious identity documents: mismatched name, SSN, or date of birth
- Medical billing complaints: whole bill is contested
- Address discrepancies

## New State Privacy Laws Impact Individuals, Health

Cont'd from pg. 1

subsequent occurrence and \$100/day for failure to report.

While a UCSF information bulletin will be sent out in the near future, UCSF continues its commitment to privacy. Both the University of California and UCSF Medical Center have existing privacy policies that are already consistent with these new laws; these state that unauthorized access, use, disclosure and viewing of medical information is unlawful and subject to sanctions and disciplinary actions up to and including termination of employment.

This means that you are already protecting patient privacy whenever you obtain, use or disclose medical information per UCSF policy and procedures. Remember to:

- Access, use, disclose only the minimum necessary
- Use safeguards to protect verbal, written, electronic health information
- Dispose of health information appropriately
- De-identify information whenever possible
- Protect your password(s), log off promptly and use computing device security
- Report promptly suspected privacy violations to the UCSF Privacy Office 415-353-2750
- Report promptly any suspected loss or theft computers by calling UCSF Police Department at 415-476-1414.

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

AB-211: [http://www.leginfo.ca.gov/cgi-bin/postquery?bill\\_number=ab\\_211&sess=CUR&house=B&author=jones](http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=ab_211&sess=CUR&house=B&author=jones)

SB-541: [http://www.leginfo.ca.gov/cgi-bin/postquery?bill\\_number=sb\\_541&sess=CUR&house=B&author=alquist](http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=sb_541&sess=CUR&house=B&author=alquist)

## Privacy Office Web Site

For further information related to privacy guidance, please visit the UCSF "Privacy Office" website which also includes privacy guidance, policies, forms as well as educational modules related to HIPAA training and FAQs at <http://hipaa.ucsf.edu> or contact the Privacy Office at 353-2750.

## OCR Guidance Documents

In October, the Office of Civil Rights released two pieces of guidance; one for patients, *When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved In Your Care* and one for providers *Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care*. Some staff and faculty mistakenly interpreted these documents to indicate we could be less stringent in how we use and disclose Protected Health Information. This is not the case. UCSF has determined that our current privacy protection policies are the best practice and should remain unchanged.

*When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved In Your Care* and one for providers *Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care*.

## Important Reminders

**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