California Confidentiality of Medical Information Act
Medical Privacy Enforcement

California Office of Health Information Integrity
The enactment of AB 211 establishes the California Office of Health Information Integrity (CalOHII) to ensure the enforcement of state law mandating the confidentiality of medical information and to impose administrative fines for the unauthorized use of medical information. CalOHII may also recommend further action be taken by various agencies or entities to impose administrative fines, civil penalties, or other disciplinary actions against persons or entities that violate state confidentiality of medical information laws. AB 211 grants CalOHII the authority to adopt, amend, or repeal such rules and regulations as may be reasonable and proper to carry out the purposes and intent of the bill.

Health Care Provider Requirements
AB 211 requires providers of health care as defined to establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information. AB 211 also requires providers of health care to reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use or disclosure

Providers of Health Care Requirements
REQUIREMENTS TO COMPLY WITH AB 211 AND THE CMIA

AB 211 Compliance Requirements for Providers of Health Care (Health & Safety Code Division 109, section 130203(a)0

1. Every provider of health care as defined in Civil Code sections 56.05(j) shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information.
   Every provider of health care as defined in Civil Code sections 56.05(j) shall reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use or disclosure.

2. **Determining Compliance** (**Health & Safety Code Division 109, section 130203(b))**
   In determining if a violation has occurred, CalOHii will consider the provider's:
   - ⇒ Complexity
   - ⇒ Size
   - ⇒ History of compliance
   - ⇒ Steps taken to correct and prevent detected violations from reoccurring, and
   - ⇒ Any factors beyond the provider's control that restricted the facility's ability to comply.
   - ⇒ Implementing regulations will be promulgated by CalOHII in the future.

3. **Unauthorized Access Defined (**Health & Safety Code Division 109, section 130201(e) - Civil Code Division 1, Part 2.6, Ch.1, sections 56 et seq. (see especially section 56.10))
   Unauthorized access is the inappropriate viewing of patient medical information without direct need for diagnosis, treatment, or other unlawful use not permitted by either the Confidentiality of Medical information Act (CMIA) or any other laws governing the use or disclosure of medical information.
   For details on who must comply and penalties for violations, information is available on the following pages:
   - ⇒ Providers of Health Care Who Must Comply
   - ⇒ Penalties

HEALTH CARE PROVIDERS WHO MUST COMPLY (Health & Safety Code Division 2, sections 1200 et seq.)
A provider of health care as defined in Civil Code sections 56.05(j) and 56.06 must comply. Generally, sections 56.05(j) and 56.06 encompass three types of providers of health care: health care facilities, health care professionals, and businesses who maintain medical information. The following lists are the providers of health care who must comply referenced in Civil Code sections 56.05(j) and 56.06.
Civil Code Division 1, Part 2.6, Ch.1, sections 56.05(j) & 56.06
Civil Code section 56.05(j) refers to facilities licensed pursuant to Sections 1204, 1250, 1725, or 1745 of the Health and Safety Code:

- ⇒ Primary care clinics = Community clinics, Free clinics
- ⇒ Specialty clinics = Surgical clinics, Chronic Dialysis clinics, Rehabilitation clinics, Alternative Birth centers
- ⇒ General acute care hospitals Emergency centers
- ⇒ Acute psychiatric hospitals = Skilled nursing facilities, Intermediate care facilities, Special hospitals Congregate living health facilities, Correctional treatment centers, Home health agencies, Hospices, Mobile health care units

Civil Code section 56.05(j) also refers to health care professionals licensed under: Division 2 of the Business and Professions Code, Osteopathic Initiative Act, the Chiropractive Initiative Act, or any person certified pursuant to Division 2.5 of the Health and Safety Code: Acupuncturists, Chiropractors, Dentists, EMT I, EMT II, and Paramedics, Nurses, Occupational therapists, Opticians,

Optometrists, Osteopaths, Pharmacists, Physician and surgeons, Physician assistants, Physical therapists, Psychiatric technicians, Psychologists, Social workers, Therapists, Vocational nurses

Licensed professionals: Business & Professions Code Division 2, sections 500 et seq.
Osteopaths: Business & Professions Code Division 2, Ch.5, art.4, sections 2080-2099
Chiropractors: Business & Professions Code Division 2, Ch.2, art.1, sections 1000-1005
Emergency Medical Services: Health & Safety Code Division 2.5, sections 1797 et seq.

PENALTIES AND REFERRALS (CalOHII's authority: Civil Code Division 1, Part 2.6, Ch.1, sections 56.36(d) & (e), Health & Safety Code Division 109, sections 130202(a)(1) & (2), Penalties: Civil Code Division 1, Part 2.6, Ch.1, section 56.36(c))

Penalties

CalOHII may assess a penalty on providers of health care as defined in 56.05 (j) other than licensed facilities. Any administrative fine assessment by CalOHII for an unauthorized use, disclosure or access of individually identifying information will be in an amount as provided in Civil Code section 56.36. An administrative fine or civil penalty for any violation by a health care facility will be assessed by the California Department of Public Health.

a. CalOHII may assess penalties against health care professionals licensed under Division 2 of the Business and Professions Code, Osteopathic Initiative Act, the Chiropractive Initiative Act, or any person certified pursuant to Division 2.5 of the Health and Safety Code:
b. CalOHII may assess the following penalties: Providers of health care as defined, that knowingly and willfully violate a patient's medical information privacy are subject to penalties of up to:
    - ⇒ $2,500 for the first offense,
    - ⇒ $10,000 for the second offense,
    - ⇒ $25,000 for each subsequent offense.

Providers of health care as defined that violate a patient's medical information for financial gain are subject to penalties of up to:

- ⇒ $5,000 for the first offense,
- ⇒ $25,000 for the second offense,
- ⇒ $250,000 for each subsequent offense, and
- ⇒ Disgorgement of any proceeds.

Any person or entity, but not entities that are licensed facilities subject to California Department of Public Health oversight or Civil Code section 56.06 entities that negligently discloses medical information in violation of the CMIA, irrespective of damage, may be subject to an administrative fine of up to $2,500 per violation. (Civil Code Division 1, Part 2.6, Ch.1, section 56.36(c), Health & Safety Code Division 109, section 130202(a)(1))

c. When assessing a penalty, CalOHII shall consider any relevant circumstances including but not limited to the following:
    - ⇒ Good faith attempts to comply,
    - ⇒ Nature of the misconduct,
    - ⇒ Any harm done,
    - ⇒ Number of violations,
    - ⇒ Persistence of misconduct,
    - ⇒ Length of time over which the misconduct occurred,
    - ⇒ Willfulness of the misconduct, and
    - ⇒ Defendant's assets, liabilities, and net worth.

Civil Code Division 1, Part 2.6, Ch.1, section 56.36(d)

Referrals (Health & Safety Code Division 109, section 130205, Civil Code Division 1, Part 2.6, Ch.1, section 56.36(e))
The director of CalOHII may recommend to the Attorney General, district attorney, county counsel, city attorney, or city prosecutor that a civil action be brought under Civil Code section 56.36. In addition, the director of CalOHII may refer evidence of potential violations for discipline or further investigation to the relevant licensing authority who shall review all evidence submitted.

Source:
http://ohii.ca.gov/calohi/MedicalPrivacyEnforcement/ProvidersofHealthCareRequirements.aspx

CONFIDENTIALITY AGREEMENT

The Federal Health Insurance Portability Accountability Act (HIPAA) Privacy Law, the Confidentiality of Medical Information Act (California Civil Code - 56 et seq.) and the Lanterman-Petris-Short Act (California Welfare & Institutions Code - 5000 et seq.) govern the release of patient identifiable information by hospitals and other health care providers. The State Information Practices Act (California Civil Code sections 1798 et seq.) governs the acquisition and use of data that pertains to individuals. All of these laws establish protections to preserve the confidentiality of various medical and personal information and specify that such information may not be disclosed except as authorized by law or the patient or individual.

Confidential Patient Care Information includes: Any individually identifiable information in possession or derived from a provider of health care regarding a patient's medical history, mental, or physical condition or treatment, as well as the patients and/or their family members records, test results, conversations, research records and financial information. Examples include, but are not limited to:

- Physical medical and psychiatric records including paper, photo, video, diagnostic and therapeutic reports, laboratory and pathology samples;
- Patient insurance and billing records;
- Mainframe and department based computerized patient data and alphanumeric radio pager messages;
- Visual observation of patients receiving medical care or accessing services; and
- Verbal information provided by or about a patient.

Confidential Employee and Business Information include, but are not limited to, the following:

- Employee home telephone number and address;
- Spouse or other relative names;
- Social Security number or income tax withholding records;
- Information related to evaluation of performance;
- Other such information obtained from the University's records which if disclosed, would constitute an unwarranted invasion of privacy; or
- Disclosure of Confidential business information that would cause harm to Healthcare.

I understand and acknowledge that:

1. I shall respect and maintain the confidentiality of all discussions, deliberations, patient care records and any other information generated in connection with individual patient care, risk management and/or peer review activities.
2. It is my legal and ethical responsibility to protect the privacy, confidentiality and security of all medical records, proprietary information and other confidential information relating to Healthcare and its affiliates, including business, employment and medical information relating to our patients, members, employees and health care providers.
3. I shall only access or disseminate patient care information in the performance of my assigned duties and where required by or permitted by law, and in a manner which is consistent with officially adopted policies of Healthcare, or where no officially adopted policy exists, only with the express approval of my supervisor or designee. I shall make no voluntary disclosure of any discussion, deliberations, patient care records or any other patient care, peer review or risk management information, except to persons authorized to receive it in the conduct of Healthcare affairs.
4. Healthcare performs audits and reviews patient records in order to identify inappropriate access.
5. My user ID is recorded when I access electronic records and that I am the only one authorized to use my user ID. Use of my user ID is my responsibility whether by me or anyone else. I will only access the minimum necessary information to satisfy my job role or the need of the request.
6. I agree to discuss confidential information only in the work place and only for job related purposes and to not discuss such information outside of the work place or within hearing of other people who do not have a need to know about the information.
7. I understand that any and all references to HIV testing, such as any clinical test or laboratory test used to identify HIV, a component of HIV, or antibodies or antigens to HIV, are specifically protected under law and unauthorized release of confidential information may make me subject to legal and/or disciplinary action.
8. I understand that the law specially protects psychiatric and drug abuse records, and that unauthorized release of such information may make me subject to legal and/or disciplinary action.
9. My obligation to safeguard patient confidentiality continues after my termination of employment.

I hereby acknowledge that I have read and understand the foregoing information and that my signature below signifies my agreement to comply with the above terms. In the event of a breach or threatened breach of the Confidentiality Agreement, I acknowledge that the Physician's Office may, as applicable and as it deems appropriate, pursue disciplinary action up to and including my termination.

Print Name: _____ Signature: _____

Department: _____ Dated: _____

SECTION	Approval date:	
Office Management	Approved by:	
POLICY AND PROCEDURE	Effective date:	
Patient Confidentiality	Revision date:	

POLICY:

Confidentiality of personal medical information is protected according to state and federal guidelines. Patients have the right to privacy for dressing/undressing, physical examination, and medical consultation. Practices are in place to safeguard patient privacy. The patient's private health information shall be maintained secure and confidential in compliance with legal, accrediting and regulatory agency requirements. All member information is regarded as confidential and obtainable only to authorized persons.

PROCEDURE:

A. The primary care provider (PCP) site shall maintain confidentiality of individual patient information. Individual patient conditions or information not discussed in front of other patients or visitors, displayed or left unattended in reception and/or patient flow areas. Patient registration sign-in sheets protect patient's privacy from other patients who may also be checking-in for their appointments. Patient sign-in sheets shall collect only minimal information using no more than one (1) patient identifier such as the patient's name.

B. The PCP site shall ensure that exam rooms and dressing areas safeguard patient's right to privacy.

C. The provider/designee shall ensure that there is a system for the following:
   1. Medical records are available at each encounter and include outpatient, inpatient, referral services, and significant consultations.
   2. Medical records are accessible within the facility, or an approved health record storage facility on the facility premises.

D. Where applicable, electronic record-keeping system procedures are established to ensure patient confidentiality, prevent unauthorized access, authenticate electronic signatures, and maintain upkeep of computer systems. Security protection includes an off-site backup storage system, an image mechanism with the ability to copy documents, a mechanism to ensure that recorded input is unalterable, and file recovery procedures. Confidentiality protection may also include use of encryption, detailed user access controls, transaction logs, idle monitor screen protection and blinded files.

E. The PCP site shall ensure that medical records are not released without written, signed consent from the patient or patient's representative, identifying the specific medical information to be released. The release will indicate to whom released and for what purpose. NOTE: The PCP site shall release and furnish necessary health records without the patient's written, signed consent to coordinate the patient's care with physicians, hospitals, or other health care entities, or to coordinate payment. PCPs shall also provide at no charge to health plans and appropriate state and federal regulators without written, signed consent from the patient, prompt access or upon demand, to medical records or information for quality management or other purposes, including utilization review, audits, reviews of complaints or appeals, HEDIS and other studies within 10 days of the request unless otherwise indicated or as agreed upon.

F. Transmittal of medical records by email shall be encrypted at all times. Transmission of medical records by fax shall include a fax cover page. The fax cover page includes a confidentiality statement which requires the recipient to maintain the information in a safe, confidential and secure manner and provide instructions on what steps to take when the transmittal is received by unintended recipients.

G. The PCP site shall ensure that medical records are retained for a minimum of 10 years following patient encounter.

H. The name of the individual delegated the responsible for securing & maintaining the security of medical records at this location is: _____

MEDICAL RECORD RELEASE AUTHORIZATION

PLEASE PRINT CLEARLY

PATIENT NAME: _____

ADDRESS: _____

PHONE #:_____BIRTHDATE: _____

1. I AUTHORIZE THE USE OR DISCLOSURE OF THE ABOVE NAMED INDIVIDUAL'S HEALTH INFORMATION AS DESCRIBED BELOW:
2. The following individual or organization is authorized to make the disclosure:
   Facility/Dr. Office Name: _____
   Address: _____
   Phone #: _____
3. For the purpose of review/examination and further authorize you to provide such copies of the records as may be requested. The foregoing is subject to such limitation as indicated below:
   _____ Entire Record _____ Substance Abuse
   _____ Psychiatric/Mental Health Information _____ HIV Information
   Specific Information: _____
4. This information may be disclosed to and used by the following individual or organization:
   Facility/Dr. Office Name: _____
   Address: _____
   Phone #: _____
   Reason for request: _____
5. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke the authorization I must do so in writing and present my written revocation to the clinic. I understand that the revocation will not apply to information that has already been released in response to this authorization.
6. I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. I need not sign this form in order to ensure treatment. I understand that I may inspect or copy the information to be used or disclosed, as provided in CFR 164.524. I understand that any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules.

   This authorization will automatically expire six (6) months from the date signed, unless otherwise indicated or revoked. I understand that I may revoke this consent at any time except to the extent that action has been taken in reasonable reliance upon the document.

_____

Signature of Patient or Legal Representative Date

_____

Signature of Witness Date

It is the policy of this medical practice that we will adopt, maintain, and comply with our Notice of Privacy Practices, which shall be consistent with HIPAA and California Law.