



MARK B HORTON, MD, MSPH
Director

State of California—Health and Human Services Agency
California Department of Public Health



ARNOLD SCHWARZENEGGER
Governor

July 29, 2009

AFL 09-03

TO: Acute Psychiatric Hospitals
Alternative Birth Centers
Chronic Dialysis Clinics
Congregate Living Health Facilities
Correctional Treatment Centers
General Acute Care Hospitals
Home Health Agencies
Hospices
Intermediate Care Facilities
Intermediate Care Facilities/Developmentally Disabled
Intermediate Care Facilities/Developmentally Disabled – Habilitative
Intermediate Care Facilities/Developmentally Disabled – Nursing
Primary Care Clinics
Skilled Nursing Facilities
Special Hospitals
Surgical Clinics

SUBJECT: Unauthorized Access or Disclosure of Patient Medical Information

AUTHORITY: Senate Bill (SB) 541 (Alquist, Chapter 605, Statutes of 2008)

This letter is being sent to notify you of new legislation effective January 1, 2009, which affects all health facilities licensed by the California Department of Public Health (CDPH) Licensing and Certification (L&C) program.

SB 541 (Chapter 605, Statutes of 2008) states that all health facilities licensed pursuant to Health and Safety Code (HSC) Sections 1204, 1250, 1725, and 1745 shall prevent the unlawful or unauthorized access to, and the use or disclosure of, a patient's medical information.

The information in this All Facilities Letter (AFL) is a brief summary of a portion of SB 541, relative to unauthorized access or disclosure of patient medical information. Facilities are responsible for following all applicable laws. CDPH's failure to expressly

notify facilities of legislative changes does not relieve facilities of their responsibility for following all laws and for being aware of all legislative changes. Facilities should refer to the full text of SB 541 to ensure compliance.

Health and Safety Code section 1280.15 provides that all health facilities shall report to the California Department of Public Health, Licensing and Certification District Office, any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information no later than five (5) calendar days after the unlawful or unauthorized access, use, or disclosure **has been detected** by the health facility. Facilities should not wait until they have conducted a preliminary review to report a breach.

Misdirected internal paper records, email, or fax transmissions to another health care worker within the same facility or health care system for the purpose of coordinating care or delivery of services do not need to be reported to the department. In these circumstances, the health facility should review internal policies and procedures to determine if changes are necessary to strengthen patient privacy protections and prevent similar occurrences in the future.

When notifying the department, the facility should include the following information:

- Date and time of reported incident
- Facility name
- Facility address/location
- Facility contact person
- Name of patient(s)
- Name of the alleged violator(s)
- General information about the circumstances surrounding the breach
- Any other information needed to make the determination for an onsite investigation

In the event the health facility does not report the violation to the department within five calendar days of detecting unauthorized access to or disclosure of a patient's medical information, the department may assess the licensee of the health facility a penalty in the amount of one hundred dollars (\$100) for each day that the violation is not reported, following the initial five-day period.

CDPH may assess an administrative penalty for up to twenty-five thousand dollars (\$25,000) per patient for the unlawful or unauthorized access, use or disclosure of a patient's medical information and up to seventeen thousand five hundred dollars (\$17,500) for each subsequent violation. For purposes of the investigation, the department will consider the health facility's history of compliance with applicable law and regulations, and the extent to which the health facility detected violations and took preventative action to immediately correct and prevent violations from recurring. The department will also consider factors outside the facility's control that may have restricted the facility's ability to comply. The department may refer a violation to the Office of Health Information Integrity (OHII), pursuant to HSC Section 1280.15(h).

AFL 09-03
Page 3
July 29, 2009

The total combined penalty assessed by the department shall not exceed two hundred and fifty thousand dollars (\$250,000) for a violation of a patient's medical information and the failure to report the violation.

If the licensee disputes a determination by the department regarding the failure to prevent or failure to timely report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information, or the imposition of the penalty, the licensee may request a hearing within ten calendar days of receipt of the penalty assessment. In lieu of a dispute, the licensee may transmit to the department, seventy-five (75) percent of the total amount of the administrative penalty for each violation within thirty (30) business days of receipt of the administrative penalty.

A prior AFL discussing SB 541's provisions concerning the increase of administrative penalties assessed for Immediate Jeopardy violations has been distributed. Please refer to AFL 09-02.

If you have any questions, please contact your respective L&C District Office.

Sincerely,

Original Signed by Kathleen Billingsley, R.N.

Kathleen Billingsley, R.N.
Deputy Director
Center for Health Care Quality