

Arnold Schwarzenegger, Governor
State of California
Business, Transportation and Housing Agency

Department of Managed Health Care
980 Ninth Street, Suite 500
Sacramento, CA 95814-2725
(916) 323-0435 -Phone
(916) 323-0438 -Fax
enforcement@dmhc.ca.gov

July 19, 2005

2005 JUL 19 PM 2:12
DEPT OF
MANAGED HEALTH CARE
ACCOUNTING OFFICE

Marlene S. Ma, Counsel
Kaiser Health Plan, Inc.
Legal and Government Relations Department
One Kaiser Plaza, 21st Floor
Oakland, CA 94612

**RE: Disclosure of Private Medical Records/Information
Enforcement Matter No. 05-081**

LETTER OF AGREEMENT

The Department of Managed Health Care's Office of Enforcement (the "Department") has completed its investigation related to the violation by Kaiser Foundation Health Plan, Inc. (the "Plan" or "Kaiser") of Health and Safety Code section 1386(b)(15). Specifically, the Department has concluded that Kaiser is culpable for its unauthorized disclosure of patient health information ("PHI") for an unknown period of time, on a publicly viewable website it created and maintained for four and one-half years in violation of the California Medical Information Act and the Knox-Keene Act.

Health and Safety Code section 1386(b)(15) states that grounds for discipline exist for a Plan's violation of the Confidentiality of Medical Information Act ("CMIA"). (Civil Code § 56 *et seq.*) With certain limited exceptions, none instantly applicable, the CMIA provides that "No...health care service plan...shall disclose medical information regarding a patient...or enrollee or subscriber of a health care service plan without first obtaining an authorization..." (Civil Code § 56.10) Medical information is defined as "any individually identifiable information, in electronic or physical form...regarding a patient's medical history, mental or physical condition, or treatment." (Civil Code § 56.05(g).)

On January 6, 2005, the Office of Civil Rights ("OCR") informed Kaiser's Northern California Privacy Office of a publicly-accessible website that contained PHI. At that time, the OCR informed Kaiser that it would not be conducting an investigation into the

matter. Nearly three (3) months later, during March 2005, Kaiser representatives notified the Department of Managed Health Care of an inadvertent disclosure of PHI.

The Department's investigation revealed that Kaiser was responsible for the creation of a website that exposed, without prior authorization, PHI to the general public. At least four (4) web pages contained an enrollee's name, address, phone number, medical record number, lab test, and lab test results. Approximately 150 additional patient names appeared throughout the website. It is noted that the subject website was utilized over a four (4) year period and that Kaiser cannot determine when the PHI was posted on the website, therefore, the amount of private-medical information exposed during that time period is unknown. The unauthorized disclosure of PHI on at least four (4) web pages reveals that Kaiser's privacy policies and procedures were disregarded.

Also, during part of the time the website was publicly viewable, Kaiser was subject to the HIPAA privacy compliance deadline of April 2003. The HIPAA privacy deadline should have resulted in the removal of the PHI, installation of security mechanisms to protect the PHI on the subject website, or the dismantling of the website. Additionally, Kaiser was assessed an administrative fine of \$25,000 in 2001 for unauthorized patient information dissemination. The gravity of Kaiser's current violation is related to the fact that PHI in electronic form has the potential of being quickly disseminated. This harm was realized when a former Kaiser employee mirrored the Kaiser website and reposted it to at least three new websites. Had Kaiser not violated the Knox-Keene Act, the former employee would not have had the opportunity to further disseminate confidential PHI.

It is noted that it was Kaiser's Information Technology ("IT") staff, those very knowledgeable about internet security and the privacy requirements allocated to patient health information, who created, used and maintained the publicly-viewable website. The evidence demonstrates that the website was opened in 1999 and only dismantled sometime in March 2005. Additionally, the explanation that the IT staff was using an unprotected website as a means to test the efficiency and cost benefits of using such a site without removal of the PHI or installation of security mechanisms to protect the confidentiality of PHI is untenable in comparison with Kaiser's obligation to protect PHI as confidential. In sum, the release of sensitive medical information is a serious breach of consumers' trust, and licensees that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information.

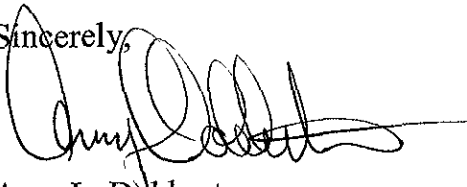
Marlene S. Ma

7/18/2005

Page 3

Kaiser has acknowledged its violation of the above-referenced section of the Health and Safety Code. The Department has determined that an administrative penalty of two hundred thousand dollars (\$200,000) is warranted in this matter and Kaiser has agreed to pay the penalty.

The Department agrees that execution of this Letter of Agreement and payment of the penalty will settle this enforcement matter.

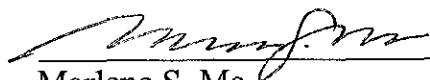
Sincerely,


Amy L. Dobberteen
Assistant Deputy Director
Office of Enforcement

TRS/kts

Accepted by Kaiser Foundation Health Plan

Date: 7.18.2005



Marlene S. Ma
Kaiser Foundation Health Plan