DEPARTMENT OF
Managed
Health Care

State Of California
Business, Transportation And Housing Agency
DEPARTMENT OF MANAGED HEALTH CARE

www.hmohelp.ca.gov

Edmund G. Brown Jr.
Governor

Edward G. Heidig
Interim Director
Department of Managed Health Care

DATE: April 7, 2011 **LETTER No. 6-K**

INFORMATION SECURITY

The purpose of this letter is to emphasize to health care service plans (health plans) their obligations to protect and secure the private medical information of their enrollees. Health plans should be taking all proactive measures necessary to ensure the security of enrollees' medical and personal information. As the use of electronic protected health information (PHI) becomes more widespread, the likelihood of unintentional breaches and disclosures also increases. The foreseeable nature of these events requires that preventative measures be taken to ensure that enrollee information is protected.

The Health Insurance Portability and Accountability Act (HIPAA) requires plans to reasonably safeguard PHI. Similarly, the Confidentiality of Medical Information Act (CMIA) obligates plans to preserve confidentiality, and penalizes plans for violations of the CMIA. See Civil Code section 56.101, for example. The Knox-Keene Health Care Service Plan Act of 1975 (Knox-Keene Act), as amended, requires health plans to file with the Department of Managed Health Care (DMHC) their policies and procedures to protect the security of patient medical information to ensure compliance with the CMIA. See Health and Safety Code section 1364.5. The DMHC is specifically authorized to take disciplinary action against a health plan for violations of the CMIA pursuant to Health and Safety Code section 1386(b)(15).

Other provisions of law also protect patients in the event of a breach of the security of medical and health insurance information. Civil Code section 1798.82 requires businesses operating in California to notify an individual, if the individual's unencrypted computerized personal information has been breached. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, also requires notification to impacted

individuals, as specified, upon a breach of any unsecured PHI including both electronic and paper records. See the federal regulations implementing these requirements located at Title 45, Code of Federal Regulations (C.F.R.), sections 164.400 through 164.414.

In light of these State and federal laws, and the increasing potential for electronic security breaches, the DMHC reminds each health plan to review, as necessary, all of its current information security policies and procedures, including those related to mobile computing devices (e.g., laptop computers), removable storage media (e.g., flash drives, external hard drives, CDs), and electronic PHI generally, for compliance with State and federal law. Each health plan should ensure that reasonable safeguards are implemented to preserve the confidentiality of any medical information maintained by the health plan, as required by the Civil Code section 56.101 of the CMIA. The health plan's review should also determine whether appropriate security breach notification protocols are in place to ensure compliance with State and federal law, in accordance with Civil Code section 1798.82, HITECH Act section 13402 and 45 C.F.R. sections 164.400 through 164.414. Health plans must file any amendments to their information security policies and procedures, as required by Health and Safety Code section 1364.5.

As a reminder, violations of the CMIA may result in penalties under the Knox-Keene Act, as well as civil and criminal penalties under the CMIA. Moreover, section 13410(a) of the HITECH Act strengthens the enforcement of violations of HIPAA, including significant increases to the civil penalties that may be imposed by the Secretary of the federal Department of Health and Human Services. See 45 C.F.R. sections 160.401 through 160.420. Section 13410(d) of the HITECH Act also allows State Attorneys General to pursue civil actions for HIPAA violations.

To help ensure the protection of enrollees' privacy interests, the DMHC will receive health plans reports on information security breaches at enforcement@dmhc.ca.gov.

Edward G. Heidig, Interim Director

By _____

Timothy L. Le Bas
Assistant Deputy Director
916) 322-6727