

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



California
Department of
Health Services
SANDRA SHEWRY
Director



ARNOLD SCHWARZENEGGER
Governor

DATE **APR 13 2006**

TO ALL HEALTH PLANS **MMCD All PLAN Letter 06001**

SUBJECT: **HIPAA REQUIREMENTS: NOTICE OF PRIVACY PRACTICES AND NOTIFICATION OF BREACHES**

Purpose:

This letter is to remind Medi-Cal Managed Care Division (MMCD) contracted Health Plans (PLAN) of their contractual responsibilities, under the Health Insurance Portability and Accountability Act (HIPAA) section of their contracts regarding:

Notify Enrollees about the Availability of Notice of Privacy Practices

The Privacy Rule requires a PLAN to remind enrollees of the availability of its Notice of Privacy Practices (NPP), as well as how to obtain a copy, no less frequently than once every 3 years.

PLAN may satisfy this requirement in a number of ways, including by:

- Sending a copy of their NPP to all enrollees.
- Mailing only a reminder concerning the availability of the NPP and information on how to obtain a copy.
- Including in a plan-produced newsletter or other publication information about the availability of the NPP and how to obtain a copy.

PLANS, other than small health plans, were first required to distribute their NPP to subscribers and enrollees by April 14, 2003. Thus, those health plans that have not already reminded subscribers and enrollees in some manner of the availability of their NPP and how they may obtain a copy, must do so no later than April 14, 2006.

Notice of Privacy Practices – California Department of Health Services (CDHS) Contact Information

PLAN must produce a NPP in accordance with standards and requirements of HIPAA that includes the CDHS Privacy Officer contact information. This contact is an alternative means for Medi-Cal beneficiaries to lodge privacy complaints.

If the PLAN maintains a website that provides information about the PLAN's services or benefits, PLAN must prominently post its notice on the website and make the notice available electronically through the web site. The address for the CDHS Privacy Officer changed in 2005. The PLAN must update their NPP to reflect the current address of the CDHS Privacy Officer as soon as reasonably possible:

Privacy Officer
c/o Office of Legal Services
California Department of Health Services
1501 Capitol Avenue
P.O. Box 997413, MS0010
Sacramento, CA 95899-7413

Notification of Breach

PLANS are bound by Exhibit "G" of their Medi-Cal contracts to notify CDHS of an unauthorized disclosure of protected health information (PHI) or any breach of data security, or intrusion within twenty-four (24) hours of discovery during a work week. In addition, Plan must investigate such breach, or unauthorized use or disclosure of PHI, and provide a written report of the investigation to the CDHS Privacy Officer within fifteen (15) working days of the discovery of the breach or unauthorized use.

Examples of breaches include but are not limited to:

- Stolen Laptop containing PHI.
- Business Associate of Plan wrongfully uses or discloses PHI.
- PHI from a Plan is posted on public website by disgruntled employee
- E-mail containing PHI is sent unencrypted and intercepted by an unintended third party.
Prior Authorization forms are left in employee's automobile, which is stolen.
- PHI is wrongfully faxed to an unintended recipient.
- Records containing PHI sent via courier service are lost.

Effective immediately, notice should be provided simultaneously to the CDHS contract manager and the Privacy Office, which can be reached by calling (916) 440-7840 or by e-mail at privacyofficer@dhs.ca.gov

Written reports should be modeled on the following outline:

- 1 Incident details including the date of the incident, when it was discovered and when CDHS was notified.
- 2 A complete description of the incident including:
 - a. What data elements were involved and the extent of the data involved in the breach.
 - b. Description of the person known or reasonably believed to have improperly used or disclosed PHI.
 - c. Description of where the PHI is believed to have been improperly transmitted, sent or utilized.
 - d. The cause or probable cause of the incident.
 - e. The impact of the incident such as -potential misuse of data, identity theft, etc.
 - f. Whether Civil code sections 1798.29, 1798.82, or any other federal or state laws requiring individual notifications of breaches are triggered.
 - g. The steps taken to reduce the harmful effects (mitigation).
 - h. Description of how the Plan will prevent reoccurrence of this incident in the future (corrective action plan).

All Medi-Cal Managed Care contracted health Plans are required to have in place administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI (electronic and non-electronic).

The Plan must maintain a comprehensive written privacy and information security program appropriate to the size and complexity of the Plan's operations and the nature and scope of its activities.

Your cooperation in this matter is greatly appreciated. CDHS has regulatory responsibility to monitor the PLAN's compliance with the HIPAA Privacy Rule. See 42 CFR § 438.100 and 438.224. Working together, we can ensure the protection of Medi-Cal beneficiaries' private health information.


All Plan Letter 06001

Page 4

APR 13 2006

If you have any questions, please contact your CDHS Contract Manager at (916) 449-5000 or the Privacy Office at (916) 440-7750.

Sincerely,


Vanessa M. Baird, MPRA, Chief
Medi-Cal Managed Care Division