DEPARTMENT OF
Managed
Health Care

Edmund G. Brown Jr., Governor
State of California
Health and Human Services Agency

Department of Managed Health Care
980 9th Street, Suite 500
Sacramento, CA 95814-2725
916-322-6727 - Phone
916-322-3968 - Fax

Date

Name
Address

Dear _____:

I am writing to advise you of an incident that resulted in the disclosure of your personal information. Health plans regulated by the Department of Managed Health Care (DMHC) are required to provide the DMHC periodically with current rosters of the medical providers the health plans contract with. Health plans are not supposed to include confidential or personal information in the rosters because the rosters are generally public documents subject to disclosure under the Public Record Act (PRA).

On May 16, 2014, the DMHC discovered that Blue Shield of California had inadvertently included provider Social Security numbers (SSNs) in the rosters Blue Shield provided to the DMHC in February, March and April, 2013. Because they did not recognize their error, Blue Shield did not mark the rosters as confidential or otherwise alert the DMHC to the inclusion of the SSNs. The DMHC's subsequent investigation revealed that the DMHC had produced the rosters in response to ten PRA requests made to the DMHC between March 2013 and April 2014. In addition to the SSNs, the rosters included providers' names, business addresses, business telephone numbers, medical groups, and practice areas.

As a result of this incident, the DMHC and Blue Shield have instituted additional protections to safeguard against future inadvertent disclosure of confidential personal information. The DMHC has acquired and installed data loss prevention software to scan all documents health plans submit to the DMHC via the DMHC's electronic filing system to alert the DMHC if confidential information, such as SSNs, is included. The DMHC is also working with health plans to ensure that they do not inadvertently include confidential information in otherwise public documents. Likewise, Blue Shield has comprehensively revised its procedures for preparing and submitting provider rosters to the DMHC. Blue Shield believes this new process, which includes multiple levels of data review and validation before filing documents with the DMHC, will prevent a recurrence of this type of incident.

We have no reason to believe that your personal information has been misused; however, to protect you from possible identity theft, Blue Shield is offering you a free one-year membership in Experian's ProtectMylD Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID is completely free to you. Enrolling in this program will not hurt your credit score.

To activate your complimentary one-year membership in ProtectMyID, please visit the website listed below and enter your individual activation code.

ProtectMyID Alert Web Site: http://www.protectmyid.com/redeem Your Activation Code: XXXXXXXXXXXXX

You must enroll by: XXXXXXXXXXXXX

If you prefer, you may enroll by phone by calling (877) 371-7902 (toll free) and speak with an Experian Customer Care representative.

We also recommend that you place fraud alerts on your credit files. A fraud alert makes it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you; however, it may also delay your ability to obtain credit. You may place a fraud alert on your file by calling any of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, you may contact the nationwide credit reporting agencies at:

Equifax (800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian (888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion (800) 680-7289
Fraud Victim Assistance
Division P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

If you discover any suspicious or unusual activity on your accounts or suspect fraud, you should report it immediately to your financial institutions. You may also contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website, at www.consumer.gov/idtheft, call the FTC at (877) IDTHEFT (438-4338), or write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Please keep a copy of this notice for your records. For more information on privacy protection steps, visit the Web site of the California Department of Justice, Privacy Enforcement and Protection Unit at www.privacy.ca.gov.

We sincerely apologize and regret any inconvenience this incident has caused you. If you have questions regarding this matter or need further information, please call toll free XXX-XXX-XXXX, Monday through Friday, 6AM to 6PM PST (except holidays).

Sincerely,

SARAH REAM
Privacy Officer
Office of Legal Services