Notice of Data Event

NOTICE OF DATA EVENT

Palomar Health Medical Group ("PHMG") recently became aware of an incident that may have impacted the privacy of information related to certain individuals. PHMG's investigation is ongoing and, at this time, it cannot determine the specific individuals and information that may have been impacted by the incident. PHMG is currently unaware of any actual or attempted misuse of information as a result of this incident. As it continues its investigation, PHMG will provide more information and directly notify any impacted individuals, but in the meantime, it is providing all patients with this notice to share information known about the incident and steps they may take to protect their information, should they feel it is appropriate to do so.

What Happened? On or around March 11, 2026, PHMG was alerted to suspicious activity in PHMG's third-party business associate's hosted environment that includes PHMG data. Upon learning of this incident, PHMG promptly notified this business associate of the incident, took steps to isolate its internal environment from exposure, and launched an investigation into this incident. PHMG's third-party business associate also investigated this incident and determined that an unauthorized actor gained access to certain files that included PHMG data. This incident did not impact the security of PHMG's internal systems.

What Information Was Involved? PHMG's investigation is ongoing and, at this time, it is not able to identify the specific individuals and information that may have been impacted. The categories of information that may be affected will vary by individual, but based on PHMG's best assessment at this time the categories of information could include name, address, date of birth, Social Security number, medical history information, disability information, diagnostic information, treatment information, prescription information, physician information, medical record number, health insurance information, subscriber number, health insurance group/plan number, credit/debit card number, security code/PIN number, expiration date, email address and password, and username and password.

What We Are Doing. PHMG takes the confidentiality, privacy, and security of information in its care very seriously. Upon being alerted to this suspicious activity, PHMG notified its third-party business associate of the activity and began a diligent investigation to confirm whether PHMG's network was impacted. PHMG's investigation confirmed that its network was unaffected and remains secure. PHMG is currently reviewing the results of the third-party business associate's investigation to confirm the nature and scope of the incident and information affected. PHMG will continue to evaluate its policies and procedures related to data privacy and security.

What You Can Do. Although PHMG is unaware of actual or attempted misuse of any information, PHMG is providing notice of this incident based on the information known through its investigation to date. PHMG encourages its patients, at all times, to remain vigilant against incidents of identity theft and fraud by reviewing account statements and explanation of benefits and monitoring

credit reports for unauthorized or suspicious activity. You can also review the "*Steps Individuals Can Take to Help Protect Personal Information*" below for further guidance.

For More Information. PHMG understands that individuals may have questions about the incident that are not addressed in this notice. We encourage individuals with questions about this incident to call (888) 202-4167 Monday through Friday 9:00 a.m. to 9:00 p.m. Eastern time, excluding holidays. You may also write to us at 15611 Pomerado Road, Poway, CA 92064.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to review Explanation of Benefits ("EOB") forms from your insurance carefully, looking for any services or treatments that the patient did not receive. If you suspect errors, notify your insurance carrier immediately of any problems. In the event of insurance fraud, you may be able to request a new account number from your insurance carrier.

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax

https://www.equifax.com/personal/credit-report-services/
1-888-298-0045
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788

Experian
https://www.experian.com/help/
1-888-397-3742
Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013
Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion
https://www.transunion.com/credit-help
1-800-916-8800
TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.