

## NOTICE OF DATA EVENT

Graybill Medical Group, Inc. (“Graybill”) recently became aware of an incident experienced by its affiliate, Palomar Health Medical Group (“PHMG”), that may have impacted the privacy of information related to certain residents. PHMG’s investigation is ongoing, and, at this time, it is not able to determine the specific individuals and information that may have been impacted by the incident. However, PHMG is currently unaware of any actual or attempted misuse of information in relation to the incident. PHMG will provide more information as it continues its investigation and learns more, but in the meantime it is providing all patients with this notice to share information known about the incident and steps they may take.

***What Happened?*** On or around May 5, 2024, PHMG identified suspicious activity on certain computer systems within its network. PHMG immediately launched an investigation to determine the nature and scope of the activity. The investigation is ongoing but has found that an unauthorized actor gained access to certain files within PHMG’s network from April 23, 2024, to May 5, 2024, and may have copied those files. Additionally, this incident may have caused certain files to become unrecoverable. However, PHMG is continuing its efforts to restore all files and identify the specific individuals and information that may have been impacted so it can provide individualized notice with additional information when its investigation is complete.

***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 You Can Do.*** PHMG encourages its patients, at all times, to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring credit reports for any 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 individuals may have questions about the incident that are not addressed in this notice. If you have questions, please call 888-829-5736 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern time, excluding holidays. You may also write to us at 15611 Pomerado Road, Suite 400, Poway, CA 92064.

### STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

#### **Monitor Your Accounts**

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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	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](http://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.