



Return Mail Processing
PO Box 999
Suwanee, GA 30024

147 2 49921 *****AUTO**ALL FOR AADC 926

SAMPLE A. SAMPLE - L01



APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



October 15, 2025

NOTICE OF [Extra2]

Dear Sample A. Sample:

Palomar Health Medical Group (“PHMG”) is writing to notify you of an incident that may have impacted your personal information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it’s appropriate to do so.

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 determined 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. Following the investigation, PHMG undertook a detailed review of all the files potentially impacted to determine what information was present in these files and to whom it related. You are receiving this letter because PHMG determined that your information was present in the potentially affected files. To date, we have seen no evidence of any fraudulent use of any data as a result of this event.

What Information Was Involved? The information potentially impacted by this incident includes your name and [Extra1].

What We Are Doing. PHMG takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovery of the event, PHMG conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its network environment, and conducted a comprehensive review of the information potentially affected. PHMG also notified law enforcement and enhanced its existing security protocols. PHMG continues to evaluate its policies and procedures related to data privacy and security. In addition to notifying you and law enforcement, PHMG will be notifying applicable state and federal regulators, as well as the consumer reporting agencies.

As an added precaution, PHMG is providing you with access to complimentary credit monitoring and identity restoration services for [Extra3] months through Experian. Information on these services and instructions on how to activate them may be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process as we are not permitted to enroll you in these services.

What You Can Do. PHMG encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. PHMG further encourages you to enroll in the complementary services being offered.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 1-833-931-4455 Monday through Friday from 6 am to 6 pm Pacific Time, excluding holidays. You may also write to PHMG at 15611 Pomerado Road, Suite 400, Poway, CA 92064, Attention: Privacy Department.

Sincerely,

Palomar Health Medical Group

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra3] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** January 30, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by January 30, 2026 at 1-833-931-4455 Monday - Friday, 6 am to 6 pm Pacific Time (excluding major U.S. holidays). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH EXPERIAN IDENTITYWORKS

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 to five 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. PHMG is located at 15611 Pomerado Road, Poway, CA 92064.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. PHMG is located at 15611 Pomerado Road, Poway, CA 92064.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400, and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There were 63 Rhode Island residents impacted by this event.

**Palomar Health Medical Group Reissues
Notice of Previously Reported Data Event in 2024**

POWAY, CA — October 15, 2025 — Palomar Health Medical Group (“PHMG”), on behalf of itself, Graybill Medical Group, Inc., and Pacific Accountable Care, LLC, is reissuing notice of an incident that may have impacted the privacy of information related to certain individuals. Originally issued in 2024, PHMG is providing this notice to individuals who may not have previously received it and to reinforce awareness around the data privacy incident that may have impacted the personal information of certain individuals.

What Happened?

On 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 determined that the incident did not affect Palomar Health. 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. Following the investigation, PHMG undertook a comprehensive review of all the files potentially impacted to assess the information contained therein and to whom it related, and to locate address information for all affected individuals. On September 4, 2025, PHMG finalized this review and determined that information related to current and former patients could be affected. To date, PHMG has seen no evidence of fraudulent use of any data as a result of this event.

What Information Was Involved?

The types of information impacted varies by individual but may include name, address, date of birth, Social Security number, driver’s license number, state identification number, military identification number, passport number, U.S. alien registration number, financial account information, payment card information, health savings account information, medical history, diagnostic/treatment information, biometric data, medical record number, Medicare/Medicaid identification number, patient account number, health insurance information, 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 discovery of the event, PHMG began a diligent investigation to confirm the nature and scope of the incident and information affected and took prompt steps to ensure security of its network environment. PHMG also notified law enforcement and will continue to evaluate its policies and procedures related to data privacy and security. PHMG is sending letters to impacted individuals where address information is available.

What You Can Do

Although PHMG is unaware of actual or attempted misuse of any information, PHMG is providing notice of this incident out of an abundance of caution. PHMG encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for

suspicious activity and to detect errors over the next 12 to 24 months. PHMG is providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files. The relevant contact information is below:

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

For additional information on how to protect yourself against identity theft and fraud and report any suspected incident of the same, please visit our website at <https://www.palomarhealthmedicalgroup.org/notice-of-data-breach/>

For More Information

We encourage individuals with questions about this incident to call the help line at 1-833-931-4455. Representatives are available for 90 days from the date of this notice, to assist you with questions regarding this incident, between the hours of 6 a.m. to 6 p.m. Pacific Time, Monday through Friday, excluding holidays. You may also write to PHMG at 15611 Pomerado Road, Suite 400, Poway, CA 92064, Attention: Privacy Department.

NOTICE OF DATA BREACH

Palomar Health Medical Group (“PHMG”), on behalf of itself, Graybill Medical Group, Inc. and Pacific Accountable Care, LLC, is providing notice of an incident that may have impacted the privacy of information related to certain individuals. PHMG is unaware of any actual or attempted misuse of information in relation to the incident.

What Happened? On 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 determined 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. Following the investigation, PHMG undertook a comprehensive review of all the files potentially impacted to assess the information contained therein and to whom it related, and to locate address information for all affected individuals. On September 4, 2025, PHMG finalized this review and determined that information related to you could be affected.

What Information Was Involved? The categories of information impacted will vary by individual, individual, but may include name, address, date of birth, Social Security number, driver’s license number, state identification number, military identification number, passport number, U.S. alien registration number, financial account information, payment card information, health savings account information, medical history, diagnostic/treatment information, biometric data, medical record number, Medicare/Medicaid identification number, patient account number, health insurance information, 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 1-833-931-4455 Monday through Friday from 6:00 am to 6:00 pm PT, excluding holidays. You may also write to PHMG 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 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	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
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; 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.