FuturHealth

Returned Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

October 17, 2025

Notice of Data <<Variable Text 2>>

Dear <<First Name>> <<Last Name>>,

This letter informs you of a potential data security incident that may have involved your information. This letter explains the incident, the measures taken in response, and steps you may consider taking.

What Happened? The investigation of a data security incident experienced by FuturHealth, Inc, which provides data hosting services to G-Plans, was recently concluded. The investigation determined that an unknown actor acquired certain data without authorization on or before October 16, 2024. A third-party vendor was then engaged to conduct a comprehensive review of the affected data to determine whether personal information may have been involved. That process was completed on October 13, 2025. Steps were taken to notify you of the incident as quickly as possible.

What Information Was Involved? The data involved included your name in combination with medical information that you provided as part of your subscription. Please note, this incident did **not** involve your Social Security number, driver's license number, or financial account information.

What We Are Doing: In addition to the steps described above, additional security measures have been implemented to further protect subscriber data and minimize the risk of future incidents.

What You Can Do: It is always a good idea to remain vigilant and review statements you receive from your healthcare provider. If you identify charges for services you did not receive, you should contact the healthcare provider immediately.

For More Information: If you have questions or need assistance, please call 1-833-687-1464 from 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday (excluding holidays).

Additional Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
TransUnion, P.O. Box 1000, Chester, PA 19016, 1-833-799-5355, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze

request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

Goglia Nutrition LLC (d/b/a G-Plans)'s mailing address is 2800 28th Street Suite 133 Santa Monica, California 90405-6204 and its phone number is 619-220-9009.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Washington D.C.: Washington D.C. Attorney General can be reached at: 400 S 6th Street, NW Washington, DC 20001; www.oag.dc.gov; 1-202-727-3400.