www.vmrc.net
VALLEY MOUNTAIN REGIONAL CENTER

Helping People with Developmental Disabilities Reach Their Maximum Potential

702 N. Aurora Street
P.O. Box 692290
Stockton, CA 95269-2290
(209) 473-0951
FAX (209) 473-0256

1820 Blue Gum Avenue
Modesto, CA 95358
(209) 529-2626
FAX (209) 557-2173

704 Mountain Ranch Rd. Suite 203
San Andreas, CA 95249
(209) 754-1871
FAX (209) 754-3211

November 5, 2021

Notice of Breach of Protected Health Information

Valley Mountain Regional Center (VMRC) is writing to inform you about a security incident that may have involved your personal health information. The privacy and security of your personal health information is extremely important to VMRC, which is why VMRC is reaching out to you.

What Happened:
On Wednesday, September 15, 2021, VMRC detected a malicious phishing e-mail received by several individuals. A phishing e-mail is when a cyber attacker sends a fraudulent e-mail to trick the recipient into clicking a link or downloading an attachment that often results in the attacker gaining access to the contents of an individual's e-mail box in an effort to gain sensitive information or deploy malicious software.

VMRC immediately removed the phishing e-mail from its server and began an investigation to determine whether any e-mail boxes might have been compromised. VMRC's investigation revealed fourteen e-mail boxes were compromised. After searching all emails contained within the compromised accounts, VMRC was able to determine whose personal health information may have been accessed or acquired by the unknown attacker/s. Your information may have been affected by this incident.

While VMRC has no evidence that the unknown attacker/s actually accessed, acquired or misused your information, out of an abundance of caution we are informing you of this incident so that you may take steps to protect your information and monitor your credit for any unusual activity. Please see the sheet at the end of this letter for information on what steps you can take to monitor your credit.

What Information Was Involved:
At this time, we have identified these types of information potentially compromised could include your name, address, date of birth, unique state-issued client identifier number (UCI number), telephone number, personal e-mail address, medical information such as diagnosis, medications, and other reports, and other potential unique identifier, or dates related to your services.

What We Are Doing:
After discovering this security incident, VMRC immediately removed the malicious phishing e-mail from its server to prevent other e-mail accounts from being compromised and prevent the application of malicious software. In addition, VMRC searched the impacted e-mail boxes both manually and electronically to identify all emails that contained confidential personal health information.

VMRC has identified, and is notifying, all individuals whose personal health information may have been compromised, which is why you are receiving this letter. VMRC takes security and privacy of your information seriously. To that end, VMRC is providing you with information on how you may protect your confidential information and monitor your credit as specified below.

What You Can Do:
Please keep a copy of this notice for future reference in case you become aware of any unusual activity involving your information. The recommendations on the following page may also help to protect your personal information.

Other Important Information:
For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at https://oag.ca.gov/privacy/medical-privacy.

For More Information:
If you have additional questions about this breach, please contact VMRC's Privacy Officer at **209-926-2703** or by e-mail PrivacyOfficer@VMRC.net. Please do not include your social security number or medical information in an e-mail to VMRC.

VMRC understands how important your health information is to you, and sincerely apologizes for any inconvenience this incident may cause you.

Sincerely,

Cindy Strawderman, Privacy Officer,
Valley Mountain Regional Center

Tony Anderson, Executive Director
Valley Mountain Regional Center

Steps You Can Take to Further Protect Your Information

Privacy Protection Steps Recommended by California Attorney General's Office: Please visit the privacy protection steps outlined in the Breach Help –Consumer Tips from the California Attorney General. It can be found at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf.

Fraud Alert: You may contact the below three credit bureaus directly to place a fraud alert on your credit files. 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.

Experian	(888) 397-3742, www.experian.com P.O. Box 9532, Allen, TX 95013
Equifax	(800) 525-6285, www.equifax.com P.O. Box 105069, Atlanta, GA 30348
TransUnion	(800) 680-7289, www.transunion.com P.O. Box 2000, Chester, PA 19022

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, the Department recommends you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, the California Attorney General's Office, and/or the Federal Trade Commission (the "FTC").

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 also contact one of the following three national credit reporting agencies, under the contact information noted above.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name. 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 or loans. You must separately place a security freeze on your credit file with each credit reporting agency noted above. To place a security freeze, you may be required to provide your personal information, such as name, social security number, date of birth, address information, among other information to initiate such freeze.