NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

Valley Professionals Community Health Center ("VPCHC") recently discovered an incident that may affect the security of personal information of certain individuals who received care from VPCHC facilities. We take this incident very seriously, and we have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. We are taking additional actions to strengthen the security of our email systems moving forward. VPCHC is also contacting the appropriate regulators regarding this incident.

What happened? On November 27, 2018, VPCHC became aware of suspicious activity relating to an employee email account. We immediately launched an investigation to determine what may have happened and what information may have been affected. Working together with a leading computer forensics expert, our investigation determined that an unauthorized individual or individuals accessed the email account between October 26, 2018 and November 27, 2018. Because we were unable to determine which email messages in the account may have been opened or taken by the unauthorized actor, we reviewed the contents of the email account to identify what personal information was stored within it.

What information may have been affected by this incident? On December 20, 2018, VPCHC determined that the affected email account contained, and the unauthorized actor may have had access to, information related to certain individuals who received treatment from a VPCHC facility, including the following types of information: name, address, Social Security number, date of birth, diagnosis, procedure, or treatment information, provider information, patient identification number, medical record number, information regarding payment for the receipt of health care, and in a very small number of instances, bank account, routing number, health insurance group number and/or member number.

The type of information affected varies per impacted individual. Although we cannot confirm that any individual's personal information was actually accessed, viewed, or acquired without permission, we are providing this notice out of an abundance of caution. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of patient information as a result of this incident.

How will individuals know if they are affected by this incident? VPCHC is mailing notice letters to the individuals whose protected information was contained within the affected email account and may have been accessed or acquired by an unauthorized actor. If an individual did not receive a letter but would like to know if they are affected, they may call the hotline listed below.

What is VPCHC doing? Information privacy and security are among our highest priorities. VPCHC has strict security measures to protect the information in our possession. Upon learning of this incident, we quickly changed the impacted employee email account password and notified our other employees to be on the lookout for suspicious emails. We are currently implementing additional technical safeguards as well as training and education for employees to prevent similar future incidents.

Although we are not aware of any actual or attempted misuse of any individuals' information, we are also providing the impacted individuals access to complimentary credit monitoring services as an added precaution.

Whom should individuals contact for more information? If individuals have additional questions or would like additional information, they may call our dedicated assistance line at 1-855-836-1353 (toll free), Monday through Saturday, 8:00 a.m. to 8:00 p.m., CT.

What can individuals do to protect their information?

Monitor Your Accounts.
To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

We recommend that you regularly review any Explanation of Benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111

www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.