May 29, 2020

Dear Customer,

Castro Valley Health, Inc. takes the privacy and protection of your personal information very seriously. We are writing to inform you of a recent data security incident that may have involved some personal information.

Please review the information provided in this letter for steps that you may take to protect yourself against any potential misuse of your information. If after reading this letter you continue to have questions or concerns, you may call the toll-free number at the bottom of this letter during regular business hours.

What Happened: The incident occurred when certain information about Castro Valley Health, Inc.'s patients inadvertently was transferred during 2016-2017 to a third-party website called Docker Hub. Castro Valley Health, Inc. first became aware of this incident on April 21, 2020, and promptly removed the information from the Docker Hub site. The transferred information was heavily coded and therefore not readable without significant decoding.

What Information Was Involved: The information that was transferred to the Docker Hub site included: patient names, an entry that said "Start of Care - Admission Visits," the name of the nurse, physical therapist, or speech therapist who admitted the patient, the address at which the patient visit was to occur, the patient's date of birth, medical record number, and the start of care date.

What Information Was <u>NOT</u> Involved: The information did **<u>not</u>** include Social Security numbers, driver license numbers, Tax ID numbers or bank account information. Importantly, the information also did **<u>not</u>** include clinical or diagnostic information, notes, plans or orders.

Castro Valley Health, Inc.'s Response: Castro Valley Health, Inc. began investigating the incident immediately after learning of it. We have no information indicating anyone has used any of the patient information from the Docker Hub website, or that anyone other than the person who alerted the Department of Health and Human Services to the situation ever has viewed the information.

We are taking extra steps in addition to our existing policies to safeguard your information, including renewed training and employee orientation, conducting additional internal security audits and risk assessments and enhancing our policies and procedures.

Additional Steps You May Wish To Take: Steps you may wish to take include:

1. Get current copies of your medical records from your healthcare providers and medical insurer and review them for any incorrect personal information or unauthorized treatments, procedures or prescriptions;
2. Monitor any medical notices and activity on your accounts; and
3. Place fraud alerts or credit freezes on your accounts to prevent or warn you if anyone without your authority tries to open an account in your name.

   You can check your credit reports at annualcreditreport.com from any one of the three major credit bureaus – Equifax, Experian, and TransUnion – and place a fraud alert on your credit report. Their contact information is below:

   Equifax: 1-888-548-7878

   TransUnion: 1-800-916-8800

   Experian: 1-888-397-3742

If you have reason to believe that your Medicare or Medicaid information is being improperly used, report that online or call 800-HHS-TIPS.

For More Information: We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please call 1-888-688-2497 toll-free during regular business.

Sincerely,

Castro Valley Health, Inc.