October 17, 2024

Notice of Data Security Incident

We are posting this notice to provide important information regarding a recent cybersecurity incident involving information maintained by Valleygate Dental Surgery Centers of Charlotte, Fayetteville, and the West ("Valleygate"), including Protected Health Information as defined by the Health Insurance Portability and Accountability Act. We want to provide details about the incident and let patients and others know that we continue to take significant measures to protect the information we maintain.

Valleygate detected anomalous activity on our network on November 17, 2023. We immediately took affected systems offline and engaged third-party cybersecurity specialists to help remediate the issue, restore systems and fully investigate the matter. On December 29, 2023, we posted an initial Notice of Data Security Incident to the Valleygate website, while we continued our investigation. On September 17, 2024, the investigation revealed that some information Valleygate maintains, including data about some patients, was potentially accessed by an unauthorized party. The type of patient information involved includes full names along with one or more of the following: patient identification number, provider name, medical treatment or procedure information, mental or physical condition, health insurance policy number, Medicaid or Medicare number, Social Security number, government issued identification number, financial account information, mother's maiden name, digital or electronic signature, address, date of birth, birth certificate, chart number, telephone number, fax number, and/or email address.

The investigation revealed that the unauthorized party gained access to our systems on or around November 16, 2023.

Valleygate has no evidence that any patient information has been used by an unauthorized person following the intrusion into our systems. Nevertheless, out of an abundance of caution, we wanted to make patients aware of the incident so they can take steps to protect their information if they feel it is appropriate to do so. Valleygate provided notification on October 17, 2024 to patients whose contact information it had on file. Valleygate also notified and is cooperating with law enforcement in connection to this incident.

Valleygate is committed to protecting the privacy of employee and patient data we maintain. Valleygate continues to work with cybersecurity professionals to evaluate and enhance practices and internal controls, and is taking significant steps to mitigate the risk to persons impacted by this incident.

The additional information below provides precautionary measures that persons can take to protect their information, including tips for protecting against medical identity theft and best practices in protecting against financial fraud. While we have no evidence of misuse, it is always important to remain vigilant.

If you have any questions regarding this incident, please call the dedicated and confidential toll-free response line at **855-577-8229**. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line is available 8:00am to 8:00pm ET, Monday through Friday, excluding holidays.

The privacy and security of the patient information Valleygate maintains is of the utmost importance and we sincerely regret any inconvenience this incident may cause to patients.

Sincerely,
Valleygate Dental Surgery Center of Charlotte LLC
Valleygate Dental Surgery Center of Fayetteville LLC

Valleygate Dental Surgery Center of the West LLC

Steps Individuals Can Take to Protect Personal Information

1. Protecting Your Medical Information.

The following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.