NOTICE OF DATA EVENT

ABOUT THE DATA EVENT

On or about November 1, 2021, VPN Solutions, a third-party hosting solution provider, notified various medical practices and providers, including Pediatric Associates, P.C. ("Pediatric Associates"), about an incident at VPN Solutions that may affect the privacy of certain information housed in the VPN Solutions systems. Pediatric Associates is providing notice of the incident so potentially affected individuals may take steps to better protect their personal information, should they feel it appropriate to do so.

FREQUENTLY ASKED QUESTIONS

What Happened? On or about November 1, 2021, VPN Solutions notified Pediatric Associates that malware encrypted certain data housed in portions of the VPN Solutions servers. Independent investigations into the nature and scope of the incident promptly followed and included communications with VPN Solutions. Those investigations confirmed that the incident impacted only VPN Solutions systems. VPN Solutions reported that the encryption process rendered certain data, including certain protected health information, unavailable to medical practices, providers, and patients. On December 22, 2021, VPN Solutions informed Pediatric Associates that the investigation determined that Pediatric Associates' data was not subject to any unauthorized access or acquisition. However, on or about February 15, 2022, VPN Solutions informed Pediatric Associates that the investigation was unable to determine whether its data was subject to unauthorized access as a result of the incident and the statement in its December 22, 2021 letter was wrong.

To date, VPN has not reported to Pediatric Associates whether its data was subject to unauthorized access as a result of the incident. However, Pediatric Associates seeks to notify its patients that the incident occurred and that Pediatric Associates is working diligently to understand and mitigate the impact of that incident.

What Information Was Involved? Although no confirmation that patient data was compromised has been communicated, the information potentially at risk as a result of the incident varies by individual and may include the following types of information: Name, address, date of birth, personal identification information, health insurance information, medical treatment/diagnosis information, and financial account information.

What is Pediatric Associates Doing? Information security remains one of the highest priorities for Pediatric Associates. As such, Pediatric Associates is evaluating its existing policies, procedures, and processes, including those with their third-party vendors, to determine whether additional measures are appropriate in an effort to reduce the likelihood of a similar future incident. Relevant regulatory authorities will receive notice, as required.

What You Can Do? Pediatric Associates encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity. You may also review and consider the information and resources outlined in the below "Steps Individuals Can Take to Help Protect Their Personal Information."

For More Information. Pediatric Associates wants to assure you that we take the responsibility to safeguard personal information very seriously. We deeply regret any inconvenience or concern this situation may have caused you. We understand that you may have questions that are not addressed in this notice. Should you have questions regarding this incident, you may call a dedicated assistance line at 1-833-599-2439 which is available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time. Should you have

questions about your personal health information or the provision of medical services, you should contact your medical practices and providers directly.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT THEIR PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.