

## Notification of Data Security Incident

April 23, 2026 – On or around February 25, 2026, we were notified that a business associate, Doctor Alliance, had experienced a data security incident involving unauthorized access to certain files through the Doctor Alliance web portal. According to Doctor Alliance, the unauthorized access occurred intermittently between October 31, 2025, and November 17, 2025. As a result, certain information relating to our patients may have been accessed by the unauthorized individual(s).

Upon learning of the incident, we promptly initiated an investigation and worked with Doctor Alliance to obtain additional information necessary to understand the nature and scope of the incident. On March 18, 2026, following the review and analysis of the information provided by Doctor Alliance, we determined that a limited amount of protected health information (“PHI”) belonging to our patients was potentially impacted in connection with this incident.

The information that could have been accessed by the unauthorized individual(s) may could have included one or more of the following: names, dates of birth, addresses, diagnoses, treatment plans, medications, and provider information. Importantly, there is no evidence that our network systems were compromised or subject to unauthorized access. This incident was limited to the Doctor Alliance environment.

We have promptly notified potentially affected individuals as quickly as possible via U.S. mail to their most recent address on file. In an abundance of caution, we have provided potentially impacted individuals with complimentary credit monitoring services. Additionally, in response to this incident, we are reviewing our current policies and procedures related to data security. Patients are encouraged to monitor their account statements and explanation of benefits forms for suspicious activity and to detect errors. Patients may also wish to contact the three major credit agencies to place a fraud alert on their credit report – the credit agencies’ contact information is: Equifax (888-378-4329); TransUnion (833-395-6938); and Experian (888-397-3472).

We have established a toll-free call center to answer questions about the incident and to address related concerns. The call center is available Monday through Friday from 9 AM - 9 PM Eastern Time and can be reached at **888-504-8228**. You may also contact us by writing to 101 W Renner Rd, Suite 420, Richardson, TX 75082.

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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.
- 8.

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

<b>TransUnion</b> 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>	<b>Experian</b> 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>Equifax</b> 1-888-298-0045 <a href="http://www.equifax.com">www.equifax.com</a>
---	---	--

<b>TransUnion Fraud Alert</b> P.O. Box 2000 Chester, PA 19016-2000	<b>Experian Fraud Alert</b> P.O. Box 9554 Allen, TX 75013	<b>Equifax Fraud Alert</b> P.O. Box 105069 Atlanta, GA 30348-5069
<b>TransUnion Credit Freeze</b> P.O. Box 160 Woodlyn, PA 19094	<b>Experian Credit Freeze</b> P.O. Box 9554 Allen, TX 75013	<b>Equifax Credit Freeze</b> P.O. Box 105788 Atlanta, GA 30348-5788

### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.