

NOTICE OF SERVICE PROVIDER DATA BREACH

July 21, 2026

We are posting this notice to provide information about a security incident experienced by one of our service providers, Unlimited Technology Systems, LLC (“Unlimited”), that occurred in October 2025. The issue involved certain personal information and/or protected health information (“PHI”) of our patients and related individuals. Unlimited provides practice management software to various health care organizations, including our practice.

On or around July 20, 2026, Unlimited began notifying affected individuals whose mailing address was sufficiently available. This notice is intended to provide information about the incident, Unlimited’s response, and other relevant details for affected individuals whose mailing address was not sufficiently available.

What Happened

On October 19, 2025, Unlimited discovered unauthorized activity within its commercial datacenter. Upon discovering the unauthorized activity, Unlimited worked with a leading cybersecurity forensic firm to investigate, notified law enforcement, and conducted a review of the relevant data. Through this investigation, Unlimited determined that an unauthorized party obtained certain personal information and/or PHI of some of our practice’s patients and related individuals between October 5 and 10, 2025.

What Information Was Involved

Unlimited has determined that the affected data may have included individuals’ names and personal information and/or PHI in one or more of the following categories: health insurance and patient balance information (such as insurance policy numbers or claims/benefits information), medical information (such as medical record number, dates of service, and diagnosis information), scanned documents (such as driver’s licenses or other government identification, insurance cards, and intake forms), Social Security numbers, and other personal information (such as date of birth, email, address, phone number, or demographic information). The particular type of information involved depends on the individual.

The personal information and/or PHI involved in the incident did **not** include full patient medical records, medical imaging, or financial information, such as credit card or bank account information.

What You Can Do

If you believe your personal information and/or PHI may have been affected by this issue, you may contact Unlimited’s dedicated call center at the phone number listed below for additional information about the incident and steps you can take to protect your personal information and PHI. Further, Unlimited has secured the services of Kroll to provide complimentary identity monitoring at no cost to affected individuals for two years. Please call the Unlimited call center phone number below to confirm and obtain information about the complimentary identity monitoring services Unlimited is offering.

We also encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing explanations of benefits (“EOBs”) and account statements and monitoring credit reports for any unauthorized or suspicious activity. Any such activities should be reported to the relevant insurance company or financial institutions immediately. Please see the Reference Guide below for more information on steps individuals can take to help protect their information.

For More Information – Unlimited Call Center

If you have questions, please call the Unlimited dedicated call center at **(844) 576-3063**, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

* * *

Reference Guide

Order Your Free Credit Report. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission’s (“FTC’s”) website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

Monitoring. You should always remain vigilant for incidents of fraud and identity theft by reviewing bank and payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately reporting any suspicious activity or incidents of identity theft. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft/.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. You can place fraud alerts with the three credit bureaus by phone, by mail, or online (see below). The bureau you contact will notify the other two bureaus about the fraud alert. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
1-888-378-4329

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/fraud/cen-ter.html
1-888-397-3742

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-victim-resource/place-fraud-alert
1-800-916-8800

Consider Placing a Security Freeze on Your Credit File. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. *Unlike a fraud alert, you must place a security freeze on your*

credit file at each consumer reporting agency individually.

To place a security freeze on your credit report, you must make a request to each consumer reporting agency by phone, by mail, or online (see below). The consumer reporting agencies may require proper identification prior to honoring your request, so to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
<http://www.experian.com/freeze/center.html>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze (at no charge) as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. This office can be reached at: Office of the Attorney General, The Capital, Albany, NY 12224-0341, (800) 771-7755, www.ag.ny.gov.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. This office can be reached at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov.