UNLIMITED TECHNOLOGY SYSTEMS, LLC
NOTICE OF DATA BREACH

On May 20, 2026, Unlimited Technology Systems, LLC ("Unlimited") notified us of an incident that occurred in October 2025 involving personal information, including health information, of some of our patients. Unlimited, on our behalf, began notifying individuals with known contact information on July 21, 2026 This notice is meant to provide information about the incident, Unlimited's response, and relevant information for individuals with no known mailing address whose data Unlimited believes may have been involved. If you have questions, please contact Unlimited at (844) 576-3063**,** Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Information regarding Unlimited is available on its website at https://www.unlimitedsystems.com/.

What Happened

Unlimited provides practice management software to various health care organizations, including us. On October 19, 2025, Unlimited discovered unauthorized activity within its commercial datacenter. Upon discovering the unauthorized activity, Unlimited hired a leading cybersecurity forensic firm to investigate, notified law enforcement, and conducted a review of the data involved. Through this investigation, Unlimited determined that an unauthorized actor may have obtained a copy of certain personal information between October 5 and October 10, 2025.

What Information Was Involved

Unlimited has determined that some of the data involved in the security incident may have included names and information 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 number, 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 data involved in the incident does not include full patient medical records, medical imaging, or financial information, such as credit card or bank account information.

What Unlimited is Doing

Unlimited has implemented enhanced security measures to prevent similar incidents from occurring in the future. Additionally, Unlimited has secured the services of Kroll to provide identity monitoring at no cost to affected individuals for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

For More Information

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

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for any unauthorized or suspicious activity. Any such activities should be reported to your financial institutions immediately.

We take this matter seriously and are committed to protecting the privacy and security of the information entrusted to us and our service providers.

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	**Experian Fraud Alert**	**TransUnion Fraud Alert**
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013-9544	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert
1-888-378-4329	1-888-397-3742	1-800-916-8800

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. This office can be reached at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.marylandattorneygeneral.gov.

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 Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

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.

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General. This office can be reached at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General. This office can be reached at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov.

You have the right to obtain a police report and request a security freeze 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 for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia. This office can be reached at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, www.oag.dc.gov