<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

SCAN TO ENROLL

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

<<Date>> (Format: Month Day, Year)

Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

You are receiving this letter because your information may have been involved in an October 2025 data security incident at Unlimited Technology Systems, LLC ("Unlimited"). Unlimited provides practice management software to various health care organizations and providers. Through an investigation, Unlimited determined that information belonging to you may have been accessed without authorization. While we are unaware of any attempted or actual misuse of any information involved in this incident, we are providing you with an overview of the data security incident, our response to it, the support we are offering to you, and additional measures you can take to help protect your personal information, should you find it necessary.

What Happened

On October 19, 2025, we discovered unauthorized activity within our commercial datacenter. Upon discovering the unauthorized activity, Unlimited hired a leading cybersecurity forensic firm to conduct an investigation, notified law enforcement, and conducted a review of the data involved. Through this investigation, we determined that an unauthorized actor may have obtained a copy of some of your 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 your name 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 We Are Doing

We implemented enhanced security measures to prevent similar incidents from occurring in the future. Additionally, we have secured the services of Kroll to provide identity monitoring at no cost to you 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. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services:

1. You must activate your identity monitoring services by **<<b2b_text_6 (Activation Deadline)>>**. Your Activation Code will not work after this date.
2. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: **<<b2b_text_5 (Activation Code)>>** and Your Verification ID: **<<b2b_text_4 (Verification ID)>>**

Additional information describing the offered services is also included with this letter.

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. You may also review the enclosure that follows this letter for general guidance on how to protect your personal information.

Unlimited takes this matter seriously and is committed to protecting the privacy and security of the information entrusted to us. We deeply regret any inconvenience caused by this incident and will continue to improve our system security to better support our customers, and in turn, their patients.

Sincerely,

Unlimited Technology Systems, LLC