Ariel Clinical Services
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2382

0000025

1_0000025

[redacted]

December 5, 2025

Re: Notice of Data Security Incident

Dear [redacted]

We are writing to notify you of a data security incident which may have included your information. Ariel Clinical Services values your trust and takes the privacy and security of all information within its possession very seriously. This letter contains information regarding the incident and information about steps that you can take to help protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened? On October 29, 2025 we determined some of your personal information may have been involved in a data security incident. On July 28, 2025 we experienced unusual activity related to certain employee email accounts and immediately secured the account and engaged cybersecurity specialists to conduct an investigation. The investigation determined that an unauthorized actor accessed emails from an employee's email account on July 25, 2025 and July 29, 2025; however, we did not determine if any specific emails were viewed or opened. After reviewing the emails to identify individuals whose information was in the email account, we reconciled this information with internal records to verify information so we could notify affected individuals.

What Information was Involved? The information may have included your name as well as your Social Security number, financial card number with access code, medical information and health insurance information. At this time, we have no evidence anyone's information was used to commit identify theft or fraud.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above to investigate the incident and to notify appropriate individuals, including yourself. In order to reduce the likelihood of a similar incident occurring in the future, we implemented additional measures to enhance the security of our network environment. Additionally, we are providing you with the opportunity to enroll in complimentary credit monitoring and identity protection services, including a $1,000,000 identity theft insurance policy at no charge to you. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. In addition, you can contact representatives who will work on your behalf to help resolve issues you may experience as a result of this incident. You can also enroll in the complementary services offered to you through TransUnion by using the enrollment code provided below.

To enroll in the credit monitoring and identity protection services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] Please note you must enroll within 90 days from the date of this letter.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-405-6108, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern time

We take your trust in Ariel Clinical Services and this matter very seriously. We appreciate your patience and understanding as we respond to this event.

Sincerely,

Ariel Clinical Services
2938 North Ave
Grand Junction, CO 81504

Steps You Can Take To Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: www.transunion.com/fraud-alerts.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. For TransUnion: www.transunion.com/credit-freeze.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.