<<Return Address>>

<<First Name>> <<Last Name >
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data <<Security Incident/ Breach>>

Dear <<First Name>>:

Aesto, LLC ("Aesto") provides healthcare data migration and archiving services for healthcare providers and writes with important information regarding a recent data security incident at Aesto involving some of your personal information. The privacy and security of the information we maintain is of the utmost importance to Aesto. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened? On or about December 18, 2025, Aesto experienced a network security incident that impacted a limited portion of Aesto's Amazon Web Services infrastructure.

What We Are Doing. Upon learning of the issue, Aesto commenced a prompt and thorough investigation. As part of Aesto's investigation, Aesto worked very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, on May 26, 2026, Aesto confirmed that between on or about December 2, 2025, and December 18, 2025, a limited amount of your personal information pertaining to your care, which was stored in Aesto's network, may have been accessed and/or acquired by an unauthorized actor. Aesto has no evidence that any of the information has been misused.

On June 26, 2026, Aesto notified your healthcare provider, Allied Health MSO Holdco, LLC ("Allied Health"), of this incident. On July 15, 2026, Aesto provided Allied Health with the affected data and list of impacted individuals. After review, on July 22, 2026, Allied Health confirmed the scope of the impact and secured information sufficient to effectuate notice.

What Information Was Involved? The information impacted includes your full name, as well as your <<Variable Text 2>>.

What You Can Do. We are offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services, including a $1,000,000 identity theft insurance policy, at no charge to you. These services provide you with alerts for [Service Length] 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services are provided through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in the credit monitoring and identity theft protection services at no charge to you, 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: <CODE HERE>. In order for you to receive the services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. If you need assistance with the enrollment process or have questions regarding these services, please call Cyberscout directly at 855-308-3709. The assistance line is available Monday through Friday, 8 am – 8 pm Eastern Time, excluding major U.S. holidays.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information. Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. **If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 833-918-8060.** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am – 9 pm Eastern Time (excluding major U.S. holidays). Be prepared to provide **your engagement number [redacted].**

Sincerely,
Aesto LLC
1800 International Park Drive, Suite 110
Birmingham, AL 35243

END OF LETTER PROVIDED BY AESTO LLC. FURTHER INFORMATION PROVIDED BY YOUR HEALTHCARE PROVIDER.

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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 (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 http://www.annualcreditreport.com/, calling toll-free 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

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

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.

Additional information:

California: California Attorney General can be reached at: 1300 I Street, Sacramento, CA 95814; 800-952-5225; www.oag.ca.gov/privacy

Iowa: Iowa Attorney General can be reached at: 1305 E. Walnut St., Des Moines, IA 50319; 888-777-4590; www.iowaatorneygeneral.gov

Kentucky: Kentucky Attorney General can be reached at: 700 Capitol Avenue, Suite 118, Frankfort, KY 40604; 502-696-5300; www.ag.ky.gov

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

Oregon: Oregon Attorney General can be reached at: 1162 Court St., NE, Salem, OR 97301; 877-877-9392; www.doj.state.or.us/consumer-protection

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 1-401-274-4400. The total number of Rhode Island residents receiving notification of this incident is <<#>>.

Washington D.C.: Washington D.C. Attorney General can be reached at: 400 S 6th Street, NW
Washington, DC 20001 oag.dc.gov 1-202-727-3400.