Averhealth Holdings Notifies Individuals of Data Security Incident

Averhealth Holdings, parent company of Avertest, Inc. (collectively, “Averhealth”) is committed to maintaining the privacy and security of personal information.

On January 20, 2026, we detected unusual activity in Avertest’s email environment. Upon detecting the unauthorized activity, Averhealth immediately contained the incident and commenced a prompt and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents. The investigation revealed that the unauthorized party gained access to our network between December 19, 2025, and January 21, 2026.

On May 6, 2026, we discovered that the unauthorized party had potentially accessed or acquired certain files that contained personal information, such as name, clinical information, diagnosis, digital / electronic signature, date of birth, driver’s license number, health insurance policy-related number, medical cost, medical dates of service, medical history, medical provider name, medical record number, medical treatment/procedure information, mental or physical condition, minor, patient account number, and Social Security number. Not all information was impacted for all individuals. On or about July 2, 2026, Averhealth is sending notification letters to each potentially affected individual for whom it their last known address.

We have no evidence of any identity theft or financial fraud related to this incident. However, out of an abundance of caution, Averhealth encourages impacted individuals to take actions to help protect their personal information. These actions include placing a fraud alert and/or security freeze on their credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing their financial account statements, explanation of benefits statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities. Averhealth is providing complimentary credit monitoring services for those who had their Social Security number impacted.

For further questions about this incident, or to determine if affected, individuals may contact the dedicated response line at (844) 959-7153, available Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time, excluding holidays.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

We recommend that you place a one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	***Experian***	***TransUnion***
P.O. Box 105069	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348-5069	Allen, TX 75013	P.O. Box 2000
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	www.experian.com/fraud/center.html	Chester, PA 19016
(888) 378-4329	(888) 397-3742	www.transunion.com/fraud-alerts
		(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348-5788 www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze/center.html (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze (888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.