

August 25, 2026

Notice of Data Breach

Advantage Home Health Care (“AHHC”) is notifying individuals whose information may have been involved in a recent data security incident. The security of the information entrusted to AHHC is important to us, and we want to ensure that potentially affected individuals are aware of the incident and the resources available to help protect their information.

What Happened? On June 16, 2026, AHHC became aware of a security incident in which an unauthorized third party gained access to one of our computer servers. On June 26, 2026, we learned that the unauthorized party acquired data that may have included personal information. Upon discovering the incident, we followed our incident response plans, took protective actions to stop the unauthorized activity, engaged leading security and forensic specialists, and launched an investigation. We also notified and worked with U.S. federal law enforcement. Based on our investigation, we determined that the unauthorized party originally gained access to the server on June 9, 2026, and was able to acquire certain documents and information stored on that server.

What Personal Information Is Involved? The information involved varies depending on the individual.

For patients, the information could have included first and last name, date of birth, Social Security number, address, phone number, and information about medical conditions and care received.

For current or former employees, the information could have included first and last name, date of birth, Social Security number, address, phone number, and information about employment with AHHC. If an employee is or was enrolled in the AHHC employee health plan, the additional information involved could have included health insurance information, plan enrollment information, claims information, healthcare provider information, and information regarding health benefits.

What We Are Doing. We take this incident very seriously. Upon detecting unusual activity in our IT system, we took protective actions to contain the activity. We also retained industry-leading cybersecurity specialists, scanned our environment, and implemented additional security measures. We will continue to evaluate and deploy security protocols, continuous monitoring, and staff training intended to help prevent and defend against cybersecurity threats. We also made diligent efforts to prevent the unauthorized third party from maintaining or further using or disclosing the data it acquired.

Although we are not aware that the information involved has been or will be used or misused for fraudulent purposes, we understand that individuals may have concerns. We are therefore offering eligible affected adults access to Single Bureau Credit Monitoring, a Single Bureau Credit Report, a Single Bureau Credit Score, and Cyber Monitoring services at no charge for 12 months through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Cyber monitoring looks for personal data on the dark web and alerts an enrolled individual if personally identifiable information is found online.

We are also offering parents and guardians of affected minor patients access to Cyber Monitoring services for themselves and their minor children at no charge for 12 months through Cyberscout.

Affected individuals should follow the enrollment instructions and use the unique enrollment code included in their notification letter. Because enrollment terms differ depending on whether the affected individual is an adult or a minor, individuals should refer to their notification letter for the applicable enrollment deadline and instructions.

What You Can Do. We sincerely regret any inconvenience or concern this incident may cause. If you received a notification letter, we encourage you to review the letter carefully and enroll in the complimentary monitoring services described in it.

We also encourage individuals to remain vigilant and monitor account statements, financial transactions, bills, notices, and free credit reports for potential fraud and identity theft. Any questionable or suspicious activity should be reported promptly to the appropriate financial institution, healthcare provider, insurance company, or law enforcement agency.

Individuals may place a fraud alert by contacting any one of the three major credit reporting agencies:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204).
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Identity Force.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

We also encourage you to, as always, remain vigilant and monitor your account statements, financial transactions, and free credit reports for potential fraud and identity theft, and promptly report any concerns. We suggest you regularly review bills, notices, and statements, and promptly report any questionable or suspicious activity.

For More Information. We value the trust that our patients, employees, and other individuals place in us, and we make every effort to protect and secure the information entrusted to us.

If you received a notification letter, believe you may have been affected, or have questions regarding this incident, please contact our toll-free incident response line at 1-888-398-2084, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.