LHC Group, Inc. ("LHC" or "we"), a national provider of home health and hospice healthcare services, is providing notice of a recent data security incident which may have affected the personal and/or health related information related to some of our current or past patients.

What Happened

LHC uses a third-party technology vendor to support referral management, care coordination, and clinical workflow functions related to home healthcare services.

On April 7, 2026, LHC became aware that an employee may have been the victim of a vishing (voice phishing) attack. Subsequently, LHC's vendor reported suspicious activity in their platform associated with an LHC user account. LHC immediately launched an investigation, took steps to secure its systems, worked with the vendor, enlisted the assistance of third-party forensic experts, and notified the FBI.

LHC's investigation determined that a threat actor stole credentials to access a large volume of files from the vendor's platform that contained patient Protected Health Information ("PHI"). The unauthorized access occurred from April 7, 2026, through April 15, 2026. After extensive review and data analysis, LHC began confirming identities of impacted individuals on July 9, 2026.

What Information Was Involved

The investigation determined that the threat actor accessed certain documents that contained patient personal data and PHI. The documents may have included:

- Full names, addresses, dates of birth, and demographics;
- Social Security numbers (in limited instances);
- Health information such as clinical summaries, treatment plans, diagnosis codes, dates of service, and physician or provider information;
- Health insurance information such as policy names, numbers, and plan information;
- Government identification information such as Medicare and Medicaid ID numbers;
- Financial information (in limited instances).

Not all data elements were involved for every individual.

What We Are Doing

LHC took steps to strengthen its security following the incident and minimize the risk of any similar incident in the future, including, but not limited to:

- Disabling the compromised account
- Conducting a review to check for additional areas of improvement
- Enhancing authentication requirements and monitoring
- Strengthening additional security controls

What You Can Do

We have no evidence or reason to believe that your information has been misused. However, as a precaution to protect against misuse of your health information, we will offer impacted individuals complimentary free credit monitoring and identity protection services and pay for this service for two (2) years. We have included steps on how to sign up for this free service.

Please check your explanation of benefits statements, bills and accounts to be sure they look correct. We have attached steps on how to do that. The enclosed Reference Guide contains instructions on how to help protect your information, as well as contact the U.S. Federal Trade Commission, place an alert or freeze on your Credit File, or contact your state attorney general if applicable.

For More Information

Safeguarding patient, member, and customer information remains a top priority. We regret that this incident occurred and apologize for any inconvenience or concern it may cause. If you have any questions regarding this notice or have further concerns, please feel free to call our dedicated call center toll free at 1-866-200-0905, Monday through Friday, 8 a.m. to 8 p.m. Central Time, excluding holidays.