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.

**Credit Monitoring Enrollment Instructions for Impacted Individuals**

**1. Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the of your letter. Please note, the deadline for enrollment is December 4, 2026.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-866-200-0905 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

# Reference Guide

## 1. Review Your Account Statements

As a precaution to protect against misuse of your health information, we recommend that you remain vigilant and regularly monitor the explanation of benefits statements that you receive from [us/your plan], and your bank and credit card statements, credit reports, and tax returns to check for any unfamiliar activity. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please contact your plan. If you do not regularly receive explanation of benefits statements, you may request that your plan send you these statements following the provision of any health care services in your name or plan number by contacting your plan. If you notice any suspicious activity on either your bank or credit card statement, or tax returns, please immediately contact your financial institution and/or credit card company, or relevant institution.

## 2. Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

Upon receiving your credit report, review them carefully. Look for any accounts you did not open. Look in the "inquires" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for inaccuracies in information (such as home address and Social Security number).

If you see anything that you do not understand, call the credit bureau at the telephone number of the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

## 3. Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and FTC.

If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides an interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

**Step 1: Call the companies where you know fraud occurred.**

**Step 2: Place a fraud alert and get your credit reports.**

**Step 3: Report identity theft to the FTC.**

**Step 4: You may choose to file a report with your local police department.**

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at https://www.identitytheft.gov/#/Steps, or you can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft at https://consumer.ftc.gov/features/identity-theft.

## 4. Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be a victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging your file with a fraud alert at all three bureaus.

| Credit Agency | Mailing Address | Phone Number | Website |
|---|---|---|---|
| **Equifax** | P.O. Box 105069<br>Atlanta, GA 30348-5069 | 1-888-766-0008 | www.equifax.com |
| **Experian** | P.O. Box 9554<br>Allen, TX 75013 | 1-888-397-3742 | www.experian.com |
| **TransUnion** | P.O. Box 2000<br>Chester, PA 19016 | 1-800-680-7289 | www.transunion.com |

## 5. Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file, at no cost to you, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) phone number, current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

| | Mailing Address | Phone Number | Website |
|---|---|---|---|

| Credit Agency | | | |
|---|---|---|---|
| **Equifax** | P.O. Box 105788<br>Atlanta, GA 30348 | 1-800-349-9960 | www.equifax.com |
| **Experian** | P.O. Box 9554<br>Allen, TX 75013 | 1-888-397-3742 | www.experian.com |
| **TransUnion** | P.O. Box 160<br>Woodlyn, PA 19094 | 1-800-916-8800 | www.transunion.com |

You can request a security freeze for free by contacting the credit bureaus at:

Once you have submitted your request, the credit reporting agency must place the security freeze no later than one (1) business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

**Additional Attorney General Office Identity Theft Resources.** You can obtain information from your state's Attorney General's Office about security breach response and steps you can take to help prevent identify theft. Please see the information below for states that provide these resources:

**For California Residents.** You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

**For District of Columbia Residents.** You can obtain additional identity theft information from the District of Columbia's Attorney General Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft.

**For Iowa Residents.** You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at:
Iowa Attorney General's Office
Director of Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319
Phone: 1-515-281-5926
Website: www.iowaattorneygeneral.gov

**For Maryland Residents.** You can contact the Maryland Attorney General at:
Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place,
25th Floor
Baltimore, MD 21202
Phone: 1-410-576-6491
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

**For Massachusetts Residents.** You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**For New Mexico Residents.** You have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
(2) proper identification to verify your identity; and
(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report. A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

**For New York Residents.** You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
Phone: 1-800-771-7755
Website: www.ag.ny.gov

**For North Carolina Residents.** You can obtain information about preventing and avoiding identity theft from the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000
Website: https://ncdoj.gov/
Identity Theft Link: https://ncdoj.gov/protecting-consumers/protecting-your-identity/

**For Oregon Residents.** State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Department of Justice at:
Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
Phone: 1-877-877-9392
Website: www.doj.state.or.us

**For Rhode Island Residents.** You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General at:
Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
Phone: 1-401-274-4400
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#