

Elara Caring
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



May 12, 2026

Re: [REDACTED]

Dear [REDACTED]:

We are writing to notify you of a data security incident that occurred at one of our third-party vendors that involved some of your personal information. We take very seriously the responsibility to protect the information of our patients. We are sending this letter to tell you what happened, what information was involved, what we are doing in response, and what you can do should you feel it is appropriate to do so.

What Happened?

From time to time, we use third-party vendors to assist with managing and signing documents related to our home health care services. On December 12, 2025, one of our third-party vendors notified Elara that, between November 4 and 6, 2025 and November 14 and 17, 2025, an unauthorized actor accessed and/or downloaded documents associated with Elara patients from their system. There was no impact to our systems as a result of this incident.

Once Elara was notified, we promptly conducted a comprehensive investigation to determine what information was involved and to whom it belonged so that we could notify our patients with impacted personal information. On March 12, 2026, Elara determined that personal information associated with its patients was among the documents downloaded as a result of the breach to the third-party vendor.

What Information Was Involved?

The information contained in the documents included your: [REDACTED]

What We Are Doing.

We want to assure you that we take this incident very seriously. Elara terminated its relationship with this third-party vendor. Additionally, we are conducting a thorough review of our information security policies, procedures, and controls, including those related to third-party vendors, and will implement appropriate enhancements to reduce the risk of a similar incident from occurring in the future.

We are also making resources available to those individuals whose information was involved. We are providing you with access to complimentary credit monitoring and remediation services through Cyberscout, a TransUnion company, for 24 months at no charge to you.

To enroll in credit monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within [REDACTED] 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. Please note that when signing up for the monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do.

To help protect your information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and Social Security number to establish credit and restoration assistance if you were not the one who initiated it. To receive these complimentary services, you must enroll by [REDACTED] from the date on this letter.
- It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing your online and financial accounts, credit reports, and Explanations of Benefits (“EOBs”) from your health insurers for any unauthorized activity. If you identify suspicious activity, you should contact the company that maintains the information on your behalf.
- Additional information about how to protect your identity and personal information is contained in **Attachment A** of this mailing. We encourage you to read and follow these steps as well.

For More Information.

We sincerely regret that this incident occurred and are committed to providing you with the necessary support and assistance. If you have questions, please contact the dedicated call center toll-free at [REDACTED], Monday through Friday from 8 am - 8 pm Eastern Time (excluding major U.S. holidays).

Sincerely,

Elara Caring
3010 Lyndon B. Johnson Fwy, Suite 1100
Dallas, Texas 75234

ATTACHMENT A: MORE INFORMATION ABOUT IDENTITY PROTECTION

If you suspect that you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps.

1. Obtain and Monitor Your Free Credit Report.

U.S. residents are entitled under U.S. law to one free credit report annually from each of the 3 major credit bureaus. You can obtain a free copy of your credit report by calling 1-877-322-8228, visiting www.annualcreditreport.com, or by completing an Annual Credit Report Request Form on the FTC's website at www.ftc.gov and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the 3 national credit reporting agencies. Do not contact the 3 credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully for discrepancies. Verify all information is correct. Look for any inaccuracies and/or accounts you don't recognize, or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting company.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer credit reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumerfinance.gov> or www.ftc.gov.

2. Implementing a Fraud Alert or Security Freeze on Your Credit File.

We recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any new accounts in your name. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name. To place a fraud alert, you can contact the 3 major credit bureaus at the addresses below to place a fraud alert on your credit report.

You have the right to place a "security freeze" on your credit file. A security freeze generally prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must contact the 3 credit bureaus below:

| Equifax | Experian | TransUnion |
|--|--|--|
| Consumer Fraud Division | Credit Fraud Center | TransUnion LLC |
| P.O. Box 740256 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022-2000 |
| (888) 766-0008 | (888) 397-3742 | (800) 680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

To request a security freeze, you will need to provide the following identifying information: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) If you have moved in the past five (5) years, the addresses where you have lived over those prior five years; (5) Proof of current address such as a current utility bill or telephone bill; and (6) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement

agency concerning identity theft. 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.

3. Additional Helpful Resources.

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 the Federal Trade Commission (“FTC”). If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC’s ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. You may also contact the FTC for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 600 Pennsylvania Avenue, NW, Washington, DC 20580; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5926.

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General’s Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov>

NYS Department of State’s Division of Consumer
Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

North Carolina Residents: You can obtain information from the FTC and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226 or (919) 716-6000, www.ncdoj.gov.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services. Approximately █ Rhode Island resident was impacted by this incident.

For Arkansas, Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Kansas, Kentucky, Louisiana, Michigan, Minnesota, Missouri, Montana, New Hampshire, Nevada, Ohio, Oklahoma, Pennsylvania, Puerto Rico, South Carolina, Tennessee, Texas, Washington, and Wyoming residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).