[redacted]

Elara Caring
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Elara Caring

[redacted]

June 23, 2026

Re: Notice of Data Security Incident

Dear [redacted]:

We are writing to notify you of a data security incident at Elara Caring ("Elara") 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?

We identified that an unauthorized actor accessed some of our employees' email accounts on February 11, 2026 and October 6, 2025. Upon learning this, we immediately terminated the unauthorized access to the employees' accounts and reset the employees' credentials. In this case, it appears that the goal of the unauthorized access was to redirect deposit paychecks from our employees to a fraudulent account. In the process of carrying out this attempt, the unauthorized actor accessed and acquired certain emails and files, some of which contained personal information about our patients. An investigation was also launched with the assistance of external cybersecurity experts to determine what information was involved and to whom it belonged so that we could notify patients with personal information involved. On April 17, 2026, Elara determined that your personal information was involved.

What Information Was Involved?

Based on our review of the data, the accessed emails and/or files contained your [redacted].

What We Are Doing.

We want to assure you that we take this incident very seriously. As detailed above, an investigation was launched with the assistance of cybersecurity experts. We also immediately terminated the unauthorized access and reset the employees' credentials. Additionally, we are conducting a thorough review of our information security policies, procedures, and controls, and will implement appropriate enhancements to reduce the risk of a similar incident occurring in the future.

[redacted]

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:

- 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

[redacted]

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 you 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.

California Residents: For California residents, visit the California Office of Privacy Protection (oag.ca.gov/privacy) for additional information on protection against identity theft.

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 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 [redacted] Rhode Island residents were impacted by this incident.

Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, https://www.marylandattorneygeneral.gov.

New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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	NYS Department of State's Division of Consumer Protection
(212) 416-8433	(800) 697-1220
https://ag.ny.gov	https://www.dos.ny.gov/consumerprotection

Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the FTC. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.