Betta Swanson
Chief Compliance & Privacy Officer
Elara Caring
900 Cooper St.
Jackson, MI 49202
bswanson@elara.com
612-271-0385

March 1, 2021

Gordon MacDonald, Attorney General
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

Pursuant to NH Rev Stat § 359-C:20, BW Homecare Holdings, LLC, d.b.a. Elara Caring ("Elara"), is writing to provide notification of a recent isolated security incident at that may have affected the personal information of New Hampshire residents.

On December 9, 2020, a phishing email was sent from a known external entity to two Elara employees. The intruder then gained access to a limited number of Elara employee email accounts and sent additional phishing emails from two accounts. The period of unauthorized access extended from December 9-16. Elara learned of the unauthorized access on December 9, and promptly mitigated the incident, changing passwords and denying access to the intruder as accounts were identified. Containment of the incident was completed on December 16. Elara immediately investigated this incident to learn what happened with the assistance of a leading specialist routinely retained to assist on cybersecurity incidents. This criminal activity has been reported to the FBI.

On January 1, 2021 Elara first identified that personal information of its patients and employees may have been exposed as part of the incident. Ultimately, Elara determined that the following categories of personal information were involved: name, date of birth, address, phone number, financial or bank account information, Social Security number, insurance information and account number, and driver's license number. Elara has no evidence that personal information was downloaded, accessed or misused by the intruder. The leading specialist assisting on this matter also confirmed that there was no evidence of malware, wire transactions, or unauthorized system access.

227 New Hampshire residents may have been affected by this incident. Notification letters were mailed to each affected New Hampshire resident on February 17, 2021. A sample copy of the notification letter is being provided with this correspondence.

In response to this incident, Elara is taking steps to prevent recurrence of similar incidents, and is continuing to investigate the incident. Elara completed an enterprise-wide password change and implemented multi-factor authentication for all users of its systems. In addition, Elara conducted enhanced security training for its personnel to better detect and prevent phishing scams. Elara is offering a complimentary two-year membership of Experian's IdentityWorksSM to all affected individuals, which covers all three credit bureaus. In addition, Elara engaged Experian to set up a call center to answer any questions from affected individuals regarding the incident.

Elara Caring remains committed to protecting the privacy and security of personal information it maintains. If you have any questions or need additional information, please do not hesitate to contact me at 612-271-0385 or by e-mail at bswanson@elara.com.

Very truly yours,

Elizabeth Swanson

Betta Swanson
Chief Compliance & Privacy Officer

Elara Caring

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 17, 2021

G2324-L01-0000001 T00001 P001 **********MIXED AADC 159
SAMPLE A SAMPLE - PHI GENERAL
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notification of Breach Involving Personal Medical Information

Dear Sample A Sample:

Protecting the personal and medical information of our patients is a priority at Elara Caring ("Elara"). In this regard, I am writing to inform you of an isolated incident involving your personal medical information. Although we have no evidence that your personal information has been compromised or misused in any way, in an abundance of caution we are writing to make you aware of a security incident so that you may take any necessary precautions.

What Happened?

On December 9, 2020, a phishing email was sent from a known external entity to two Elara employees. The intruder then gained access to a limited number of Elara employee email accounts and sent additional phishing emails from two accounts. The period of unauthorized access extended from December 9-16. Elara learned of the unauthorized access on December 9, and promptly mitigated the incident, changing passwords and denying access to the intruder as accounts were identified. Containment of the incident was completed on December 16. Elara immediately investigated this incident to learn what happened with the assistance of a leading specialist routinely retained to assist on cybersecurity incidents. This criminal activity has been reported to the FBI.

The FBI refers to this type of criminal activity as a Business Email Compromise (BEC)—also known as Email Account Compromise (EAC) – and it has impacted many companies in the United States and around the world.[1] In this type of phishing scheme, the email appears to come from a known source to make the message appear to be legitimate.

What Information Was Involved?

The personal medical information potentially exposed included the following: name, date of birth, address, phone number, financial or bank account information, Social Security number, insurance information and account number, and driver's license number.

[1] FBI Public Service Announcement (April 6, 2020) (Alert Number I-040620-PSA), https://www.ic3.gov/Media/Y2020/PSA200406.

There is no evidence that personal information of Elara patients was downloaded, accessed or misused by the intruder. The leading specialist assisting on this matter also confirmed that there was no evidence of malware, wire transactions, or unauthorized system access. We wanted to make you aware of this incident in an abundance of caution and so you could take steps to protect yourself.

What We Are Doing

Elara Caring takes the protection of your personal and medical information very seriously. We regularly review our systems and privacy and security practices to enhance those protections.

In response to this incident, Elara is taking steps to prevent recurrence of similar incidents, and is continuing to investigate the incident. Elara completed an enterprise-wide password change and implemented Multifactor Authentication (MFA) for all users of its systems. In addition, Elara Caring conducted enhanced security training for its personnel to better detect and prevent phishing scams.

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **May 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 704-9390 by **May 31, 2021.** Be prepared to provide engagement number **DB25466** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you have questions about the incident or believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(833) 704-9390**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find tips and information about identity protection at this site.

What You Can Do

Although we have no evidence that your information has been misused, we want to make you aware of resources you may access to help safeguard your personal information, as outlined below.

Even though we have no indication that your personal information has been used to commit fraud, we recommend that you consider taking steps to protect yourself from medical identity theft. Medical identity theft occurs when someone uses an individual's name, and sometimes other identifying information, without the individual's knowledge to obtain medical services or products, or to fraudulently bill for medical services that have not been provided. We suggest that you regularly review the explanation of benefits statements that you receive from your health plan. If you see any service that you did not receive, contact the health plan at the number on the statement.

We also recommend that you monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. You may also want to consider obtaining a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies listed below:

Equifax	**Experian**	**TransUnion**
1-866-640-2273	1-888-397-3742	1-855-681-3196
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

You may also choose to contact the three national credit reporting agencies listed above for information about placing a "fraud alert" and/or a "security freeze" on your credit report to further detect any possible misuse of your personal information. Contact the Federal Trade Commission for additional information about "fraud alerts" and "security freezes," and about how to monitor and protect your credit and finances.

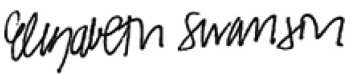
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
(202) 326-2222
www.ftc.gov

For More Information

We understand that this incident may pose an inconvenience to you, and we sincerely regret that this situation has occurred. Elara Caring is committed to protecting the privacy and security of your personal medical information, and we want to assure you that we have implemented appropriate measures to safeguard that information. We value the trust you have placed in us, and we thank you for trusting Elara Caring with your healthcare.

If you have questions or concerns about this incident, please contact Elara Caring at (855) 835-2722 or privacy@elara.com.

Very truly yours,



Betta Swanson
Chief Compliance & Privacy Officer