CONSTANGY
BROOKS, SMITH & PROPHETE LLP

January 24, 2024

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Coastal Hospice & Palliative Care ("Coastal Hospice") in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

On July 24, 2023, Coastal Hospice experienced a network disruption and immediately initiated an investigation of the matter. Coastal Hospice engaged cybersecurity experts to assist with the process. The investigation determined that certain files may have been acquired without authorization. After a thorough review of those files, on or about November 20, 2023, some personal and/or protected health information was identified as being contained within the potentially affected data. Since that time, Coastal Hospice has been coordinating to provide notice to potentially impacted individuals.

2. **Number of New Hampshire residents affected.**

Coastal Hospice notified two (2) New Hampshire residents of this incident via first class U.S. mail on January 22, 2024. A sample copy of the notification letter is included with this correspondence. The information potentially impacted in connection with this incident includes
.

3. **Steps taken relating to the Incident.**

As soon as Coastal Hospice discovered this incident, Coastal Hospice took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. Coastal Hospice implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. In addition, Coastal Hospice also notified the Federal Bureau of Investigation of the incident and will provide any cooperation necessary to help hold the perpetrator(s) accountable

Further, Coastal Hospice has established a toll-free call center through Epiq, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available Monday through Friday from 8 am – 10 pm, or Saturday and Sunday from 10 am – 7 pm, Eastern Time (excluding major U.S. holidays). In addition, while Coastal Hospice is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Coastal Hospice is also providing complimentary credit and identity protection services to notified individuals.

4. Contact information.

Coastal Hospice remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Coastal Hospice
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Date>>

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Middle Name>> <<Last Name>>:

I am writing to inform you of a data security incident that may have affected your personal and/or protected health information. At Coastal Hospice & Palliative Care ("Coastal Hospice") we take the privacy and security of all information in our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened? On July 24, 2023, Coastal Hospice experienced a network disruption and immediately initiated an investigation of the matter. We engaged cybersecurity experts to assist with the process. The investigation determined that certain files may have been acquired without authorization. After a thorough review of those files, on or about November 20, 2023, some of your personal and/or protected health information was identified as being contained within the potentially affected data. Since that time, we have been coordinating to provide notice to potentially impacted individuals, including you.

What Information Was Involved? The information may have involved your name, <<Breached Elements>>.

What Are We Doing? As soon as Coastal Hospice discovered the incident, we took the steps described above. We also implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. In addition, we notified the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators accountable.

In addition, we are offering you complimentary credit monitoring and identity protection services through Equifax. These services include of credit and dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Additional details are included at the end of this letter.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by <<Enrollment Deadline>>** (Your code will not work after this date.)
- **Visit** the Equifax website to enroll: www.equifax.com/activate
- Provide your **activation code**: **<<Activation Code>>**

What Can You Do? We recommend that you review the guidance included in this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you through Equifax by using the activation code provided above.

For More Information: Further information about how to help protect your personal information appears on the following page. In addition, Coastal Hospice has established a dedicated call center through Epiq to answer any questions about this matter and to provide assistance with enrolling in the complimentary services being offered to you. The call center can be reached at 888-541-0492 Monday through Friday from 9 am – 9 pm, Eastern Time (excluding major U.S. holidays).

Sincerely,

Monica Escalante
Coastal Hospice & Palliative Care

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. 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 prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.