David McMillan
45 Main Street
Suite 206
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

February 28, 2025

VIA ONLINE SUBMISSION
Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Bethesda Foundation d/b/a Bethesda Senior Living Communities in conjunction with the recent data security incident described in greater detail below.

1. Nature of the Security Incident

On or around September 18, 2024, Bethesda Foundation identified suspicious activity within its email system. In response, Bethesda Foundation took immediate steps to secure the email system and engaged a leading cybersecurity firm to investigate and help determine what happened. Based on the investigation, Bethesda Foundation learned that an unauthorized actor gained access to the email system between August 19, 2024 - September 18, 2024 and potentially viewed and / or downloaded certain emails. Following a comprehensive review of the potentially affected data, Bethesda Foundation determined that certain individuals' personal information may have been impacted and began working to identify up-to-date address information necessary to provide notice of the incident. Bethesda Foundation completed those efforts on February 12, 2025. On February 28, 2025, Bethesda Foundation issued notification letters to all impacted individuals with verifiable address information and provided complimentary credit monitoring and identity protection services to individuals whose Social Security numbers were affected by the incident.

2. Type of Information and Number of Nebraska Residents Notified

The information potentially accessed by the unauthorized actor included individuals' names, dates of birth, Social Security numbers, driver's license or other government-issued identification numbers, medical information and health insurance information. On February 28, 2025, Bethesda Foundation notified fifty-three (53) Nebraska residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Bethesda Foundation has implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, Bethesda Foundation has offered individuals complimentary services by Cyberscout through Identity Force, a TransUnion company. Individuals will be offered Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services, proactive fraud assistance, and access to a call center for support for 90 days.

4. Contact Information

Bethesda Foundation remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at dmcmillan@constangy.com.

Best regards,

Very truly yours,

David McMillan of
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Encl: Sample Notification Letter

Bethesda Foundation
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS415

0001453

8_0001453

BETHESDA
SENIOR LIVING COMMUNITIES

[redacted]

February 28, 2025

Subject: Notice of Data Security Incident

Dear [redacted]:

We are writing to inform you of a recent data security incident experienced by Bethesda Foundation d/b/a Bethesda Senior Living Communities that may have involved some of your personal and / or protected health information. This letter is to notify you of the incident and inform you about steps you can take to help protect your information.

What Happened: On or around September 18, 2024, we identified suspicious activity within our email system. In response, we took immediate steps to secure our email system and engaged a leading cybersecurity firm to investigate and help us determine what happened. Based on this investigation, we learned that an unauthorized actor gained access to our email system between August 19, 2024 - September 18, 2024 and potentially viewed and / or downloaded certain emails. Following a comprehensive review of the potentially affected data, we determined that your personal and / or protected health information may have been impacted by this incident. We then worked diligently to identify up-to-date address information necessary to provide notice to you.

What Information Was Involved: The information that was potentially downloaded by the unauthorized party may have included your name as well as the following: Date of Birth, Social Security Number, Financial Account Number, Medical Record Number (MRN), Patient Account Number (PAN), Medicaid Number, Health Insurance Account/Member Number, Health Insurance Group Number, Medical Diagnosis Information, Medical Treatment/Procedure Information, Clinical Information, Prescription Information, Provider Location, Provider Name. Please note that we have no evidence that your information has been misused.

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures. We are also providing you with information about steps that you can take to help protect your information.

We are also providing you with the opportunity to enroll in Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge to you. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate 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 90 days 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 monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. We also encourage you to enroll in the complementary services being offered to you through Cyberscout by using the enrollment code provided above.

For More Information: Further information about how to protect your information appears on the following page. If you have questions or need assistance, please call Cyberscout at 1-833-799-3806 from 8:00 A.M. to 8:00 P.M. Mountain Time, Monday through Friday (excluding holidays). Cyberscout call center representatives are fully versed on this incident and can answer any questions that you may have.

The security of your information is a top priority for Bethesda Senior Living Communities. We value your trust in us and take this matter very seriously. We deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Austin Harbach
Vice President of Legal Services
Bethesda Senior Living Communities

0001453

Steps You Can Take to Protect Your Personal 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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-888-378-4329	1-800-831-5614	1-800-916-8800
www.equifax.com	www.experian.com	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
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.