MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeff Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Wayne, PA 19087

September 18, 2020

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Mount Sinai South Nassau ("South Nassau"), located at One Healthy Way, Oceanside, NY 11572. South Nassau is writing to notify your office of an incident that may impact the privacy of personal information relating to one (1) New Hampshire resident. South Nassau reserves the right to supplement this notice with new significant facts learned subsequent to its submission By providing this notice, South Nassau does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On Thursday, July 16, 2020, South Nassau received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management tools to non-profit organizations, including South Nassau.

Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic consultants to investigate. Following its investigation, Blackbaud notified its customers, including South Nassau, that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, South Nassau immediately commenced an investigation

to determine what, if any, sensitive South Nassau data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On August 28, 2020, South Nassau's investigation determined that the information potentially affected may have contained personal information.

The investigation determined that, in addition to first and last names, one or more of the following types of information related to New Hampshire residents may have been accessible within the affected systems: Name and medical information. To date, the investigation has found no evidence of any actual or attempted misuse of personal information as a result of this event.

Notice to New Hampshire Residents

On September 18, 2020, South Nassau provided written notice of this incident to potentially affected individuals. This includes approximately one (1) New Hampshire resident whose personal information under state law may have been accessible. Written notice to the individual is being provided in substantially the same form as the letter attached here as ***Exhibit A***. South Nassau also placed notice of this incident on its website.

Other Steps Taken and To Be Taken

Upon learning of this incident, South Nassau moved quickly to assess the security of its potentially affected data and to notify potentially impacted individuals. South Nassau is also offering contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident.

Additionally, South Nassau is providing affected individuals with guidance on how to better protect themselves against identity theft and fraud. This guidance includes information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant about incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, the respective state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. South Nassau will also be providing notice of this event to other regulators as may be required under applicable state law.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4784.

Very truly yours,

Jeff Boogay of
MULLEN COUGHLIN LLC

JJB/hyb
Enclosure

EXHIBIT A

Mount Sinai South Nassau

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Mount Sinai South Nassau ("South Nassau") writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, South Nassau received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management tools to non-profit organizations, including South Nassau. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on South Nassau data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic consultants to investigate. Following its investigation, Blackbaud notified its customers, including South Nassau, that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, South Nassau immediately commenced an investigation to determine what, if any, sensitive South Nassau data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On August 28, 2020, South Nassau's investigation determined that the information potentially affected may have contained personal information.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained a reference in a donation made to South Nassau, by you or in your name, which identified you as a patient. The impacted information did not contain your Social Security Number, financial account information, payment card information or driver's license number. Please note that, to date, we have not received any information from Blackbaud that your information was specifically accessed or acquired by the unknown actor, but this possibility could not be ruled out.

What Are We Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying certain state regulators, as required. Additionally, while we are unaware of any actual or attempted misuse of your information, in an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take further steps to protect your information, should you feel it appropriate to do so.

What Can You Do. We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information.* There you will find general information on what you can do to help protect your personal information.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-???-???-???? Monday through Friday between the hours of 9:00 am and 6:30 pm Eastern Time (excluding holidays). You may also write to Mount Sinai South Nassau at: One Healthy Way, Oceanside, NY 11572.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Timothy Matejka

Timothy Matejka
Executive Director of Development
Mount Sinai South Nassau

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three (3) major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following 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, provide the addresses where you have lived over the prior five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
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 a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain

further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us.

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

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov.

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 1 Rhode Island resident(s) impacted by this incident.