LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

May 7, 2020

VIA ELECTRONIC SUBMISSION
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent Moorestown Visiting Nurse Association ("Moorestown VNA"), a not-for-profit community hospital, located in Moorestown, New Jersey regarding a recent data security incident described in greater detail below.

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

On March 19, 2020, Moorestown VNA was notified by Crossroads Technologies, a vendor who provides data hosting, that they had experienced a ransomware attack, and that after conducting an investigation, they believed that Moorestown VNA's patient database was accessible by the ransomware attacker. Moorestown VNA began an investigation to determine what patients' information may have been stored in the impacted data base so that notification could be sent to any potentially impacted individuals. The information that may have been accessible by the ransomware attacker includes patient names, addresses, dates of birth, Social Security numbers, patient ID numbers, and medical records.

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

Moorestown VNA notified one (1) New Hampshire resident of this data security incident via first class U.S. mail on May 7, 2020. A sample copy of the notification letter is included with this correspondence.

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

Moorestown VNA has been informed by Crossroads Technologies that they have deployed monitoring tools on their systems, reset password, and notified the FBI. Moorestown VNA is also

evaluating its relationship with Crossroads Technologies to ensure that the information they store for us is safe and protected.

Moorestown VNA has established a toll-free call center through Kroll to answer any questions about the incident and address related concerns. The call center is available Monday through Friday from 9:00 am to 6:30 pm Eastern Standard Time at 1-866-377-0067. In addition, while Moorestown VNA is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Moorestown VNA is also providing twelve (12) months of complimentary credit monitoring and identity theft protection services to the impacted individuals. In addition, Moorestown VNA has notified the three major consumer reporting agencies about the incident.

4. Contact information.

Moorestown VNA 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 me at 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Best regards,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN
Enclosure

MOORESTOWN
VISITING NURSE ASSOCIATION

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

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

Subject: Notification of Data Security Incident

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

We are writing to inform you of a data security incident that may have affected some of your personal health information. The privacy and security of your information is extremely important to Moorestown Visiting Nurse Association ("MVNA"). That is why we are writing to inform you about this incident, offer you complimentary identity monitoring services, and provide you with information relating to steps that can be taken to help protect your information.

What Happened? MVNA has been notified by Crossroads Technologies, a vendor who provides data hosting, that it experienced a ransomware attack on November 29, 2019. On March 19, 2020, Crossroads Technologies confirmed that after conducting an investigation, they believe that our patient database was accessible by the ransomware attacker. While we have no evidence to suggest that your information has been misused, out of an abundance of caution, we are writing to inform you of the incident and to provide you with access to complimentary identity monitoring services.

What Information Was Involved? The information that may have been accessible by the ransomware attacker includes patient names, addresses, dates of birth, Social Security numbers, patient ID numbers, and medical records.

What Are We Doing? As soon as we were notified by Crossroads about the incident, we retained cybersecurity experts to assist us with assessing this situation, and we began the process to gather information so we could notify potentially impacted patients. In addition, we are offering you one year of complimentary identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response. These services include Credit Monitoring, a $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **August 7, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive these services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What Can You Do? We recommend that you activate your complimentary Kroll services. We also recommend that you review the information we are providing with this letter about steps you can take to help safeguard your personal information.

For More Information: If you have questions or need assistance, please call 1-866-377-0067 from Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Sean Rabindranauth
Moorestown Visiting Nurse Association

Steps You Can Take to Further 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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.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: Under U.S. law, 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. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General **Bureau of Internet and Technology Resources** 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	**Maryland Attorney General** 200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	**North Carolina Attorney General** 9001 Mail Service Center Raleigh, NC 27699 www.ncdoj.gov 1-877-566-7226	**Rhode Island Attorney General** 150 South Main Street Providence, RI 02903 www.riag.ri.gov 401-274-4400

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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

Kroll | A Division of DUFF & PHELPS

As referenced above, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services[1] include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **August 7, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

If you have questions, please call 1-866-377-0067, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Take Advantage of Your Services

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.