Richard A. Berger, MD
4300 Alton Rd #2070
Miami Beach, FL 33140

January 20, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Richard A. Berger, MD – Incident Notification

Dear Sir or Madam:

I am writing to provide notification of an incident at Richard A. Berger, MD that may affect the security of personal information of approximately two (2) New Hampshire residents. Richard A. Berger, MD's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Richard A. Berger, MD does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On March 1, 2020, a backup drive utilized by Richard A. Berger, MD was determined to be infected with ransomware that encrypted files stored on the drive. Upon learning of the issue, Richard A. Berger, MD immediately commenced a prompt and thorough investigation. After an extensive forensic investigation and comprehensive manual document review, Richard A. Berger, MD discovered on November 30, 2020 that the impacted data contained the residents' personal and/or protected health information. The impacted data contained the affected residents' full names and Social Security numbers.

To date, Richard A. Berger, MD has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, Richard A. Berger, MD wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Richard A. Berger, MD is providing the affected residents with written notification of this incident on January 20, 2021 in substantially the same form as the letter attached hereto. Richard A. Berger, MD offered the affected residents a complimentary one-year membership with a credit monitoring service. Richard A. Berger, MD advised the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents were also provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. The affected residents are also being provided steps to take to safeguard against medical identity theft.

At Richard A. Berger, MD, protecting the privacy of personal information is a top priority. Richard A. Berger, MD is committed to maintaining the privacy of personal information

in its possession and has taken many precautions to safeguard it. Richard A. Berger, MD continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Richard A. Berger, MD provided notification to individuals pursuant to the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

Should you have any questions regarding this notification, please contact me at (305) 674-2609. Thank you for your cooperation.

Sincerely,

Richard Berger, MD

Richard Berger, MD

Encl.

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Richard A. Berger, MD. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On March 1, 2020, a backup drive utilized by Richard A. Berger, MD was determined to be infected with ransomware that encrypted files stored on the drive.

What We Are Doing.

Upon learning of the issue, we immediately commenced a prompt and thorough investigation. After an extensive forensic investigation and comprehensive manual document review, we discovered on November 30, 2020 that the impacted data contained some of your personal and/or protected health information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The impacted information included some of your personal and/or protected health information, including your [redacted].

What You Can Do.

To protect you from potential misuse of your information, we are offering you a complimentary one-year membership in Equifax® Credit Watch™ Silver. For more information on identity theft prevention and Equifax® Credit Watch™, including instructions on how to activate your one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis. We have also provided information on protecting your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. Since the date of this incident, we have implemented additional technical safeguards to safeguard information and have educated our workforce members on identifying and responding to security incidents.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern Time.

Sincerely,

Richard A. Berger, MD

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

EQUIFAX®

Enter your Activation Code: [redacted]

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service Equifax® Credit Watch™ Silver for one year. **You must enroll by** [redacted] (your code will not work after this date).

Product Information

Equifax® Credit Watch™ Silver provides you with the following key features:

- Equifax credit file monitoring with alerts to key changes to your Equifax Credit Report.
- Automatic Fraud Alerts.[1] With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit.
- Wireless alerts (available online only). Data charges may apply.
- Access to one Equifax® credit report.
- Up to $25,000 Identity Theft Insurance.[2]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to [redacted]

1. Welcome Page: Enter the Activation Code provided at the top of this page in "Activation Code" and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, review the Terms of Use and then check the box to accept and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

2. Consider Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

[1] The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[2] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

6. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.