McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

April 9, 2021

VIA U.S. MAIL

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

Re: Crystal Lake Clinic PC – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Crystal Lake Clinic PC ("Crystal Lake Clinic"). I am writing to provide notification of an incident at Crystal Lake Clinic that may affect the security of personal information of three (3) New Hampshire residents. Crystal Lake Clinic'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, Crystal Lake Clinic does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On August 26, 2020, Crystal Lake Clinic became aware of a malware incident that had infected a number of its systems and encrypted files on several machines. In addition to encrypting files, an unauthorized party may have removed a limited number of files and folders from their system. Crystal Lake Clinic immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate these types of situations. Based on its comprehensive investigation and manual document review, Crystal Lake Clinic discovered on February 10, 2021 that the impacted data included limited amounts of personal information, including the affected residents' full name, driver's license or state identification number, clinical information, medical treatment/procedure information, health insurance account number, and health insurance group number.

To date, Crystal Lake Clinic has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, Crystal Lake Clinic 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. Crystal Lake Clinic is providing the affected residents with written notification of this incident commencing on or about April 9, 2021, in substantially the same form as the letter attached hereto. Crystal Lake Clinic is advising 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 are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. Crystal

Lake Clinic is also providing the affected residents with steps to take to safeguard themselves against medical identity theft.

At Crystal Lake Clinic, protecting the privacy of personal information is a top priority. Crystal Lake Clinic is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Crystal Lake Clinic continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Notification of this matter has also been provided to the U.S. Department of Health and Human Services Office for Civil Rights, in compliance with 45 CFR §§ 164.400-414. Crystal Lake Clinic operates as a covered entity, and data relating to the New Hampshire residents was subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

J
James J. Giszczak

Encl.

CRYSTAL LAKE HEALTH CENTER

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

[redacted]

Dear [redacted]:

The privacy and security of your personal information is of the utmost importance to Crystal Lake Clinic PC ("Crystal Lake Clinic"). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

On August 26, 2020 we became aware of a malware incident that had infected a number of our systems and encrypted files on several machines. In addition to encrypting files, an unauthorized party may have removed a limited number of files and folders from our system.

What We Are Doing.

Upon learning of the issue, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents. The investigation worked to identify what personal information, if any, might have been present in those encrypted files. After an analysis of those files, we discovered on February 10, 2021 that certain elements of your personal data were present in the encrypted files. While we have no indication or evidence that any of that data has been or will be misused, we thought it important to notify you of this incident.

What Information Was Involved?

The impacted files contained some of your personal information and/or protected health information, specifically your [redacted].

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Nevertheless, we wanted to make you aware of the incident. This letter also provides 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 financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we have also provided guidance on protecting your medical and/or health insurance information.

For More Information.

Please accept our sincere 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.

If you have any further questions regarding this incident, please call our toll free response line at [redacted]. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Crystal Lake Clinic PC

– OTHER IMPORTANT INFORMATION –

1. 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
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

2. 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
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
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.

3. 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.

4. 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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

5. Protecting Your Medical Information.

If this notice letter states that your medical information was impacted, 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.