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

Dominic A. Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

May 18, 2020

VIA U.S. MAIL

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

Re: Advanced Urgent Care – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Advanced Urgent Care. I am writing to provide notification of an incident at Advanced Urgent Care that may affect the security of personal information of one (1) New Hampshire resident. Advanced Urgent Care'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, Advanced Urgent Care does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On March 1, 2020, Advanced Urgent Care detected that a ransomware incident impacted a limited number of computer files. Upon learning of the issue, Advanced Urgent Care immediately commenced a prompt and thorough investigation. As part of its investigation, Advanced Urgent Care has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. On March 9, 2020, Advanced Urgent Care determined that the threat actor group behind the ransomware attack acquired certain files containing patient data. The exfiltrated data contained the affected resident's full name and Social Security number.

To date, Advanced Urgent Care has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, Advanced Urgent Care wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Advanced Urgent Care provided the affected resident with written notification of this incident on May 8, 2020 in substantially the same form as the letter attached hereto. Advanced Urgent Care offered the affected resident a complimentary one-year membership with a credit monitoring service. Advanced Urgent Care advised the affected resident about the process for placing fraud alerts and/or security freezes on his/her credit files and obtaining free credit reports. The affected resident was also provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Advanced Urgent Care 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 (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

1709 Atlantic Blvd.
Key West, FL 33040

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 Advanced Urgent Care. 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, we detected that a ransomware incident impacted a limited number of computer files. On March 9, 2020, we determined that the threat actor group behind the ransomware attack acquired certain files containing patient data.

What We Are Doing.

Upon learning of the issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The exfiltrated data contained some of your personal and 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 protected health information, including your full name, address, Social Security number and one or more of the following: phone number, internal account number, date of service, medical provider, medical billing information and health insurance information.

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 WatchTM Silver. For more information on identity theft prevention and Equifax® Credit WatchTM Silver, 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.

If you have any further questions regarding this incident, please call [redacted] at [redacted], Monday to Friday, 9:00 a.m. to 5:00 p.m.

Sincerely,

Advanced Urgent Care

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring

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

Enrollment Instructions

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

1. Welcome Page: Enter the following Activation Code [redacted] in the "Activation Code" box 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.

Identity Restoration

In the event that you become victim of identity theft, you will receive Equifax Identity Restoration by calling [redacted], 9:00 a.m. to 8:00 p.m. Eastern, Monday through Friday, before [redacted]. An Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Please keep a copy of this letter to provide as proof of eligibility to receive Equifax Identity Restoration.

[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.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "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

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.

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.