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

September 9, 2020

VIA U.S. MAIL

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Inova Health System – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Inova Health System ("Inova"). I am writing to provide notification of an incident that may affect the security of personal information of approximately two thousand four hundred seventy (2,470) Washington residents. Inova'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, Inova does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

On July 16, 2020, Inova was notified by Blackbaud, a third party service provider used for fundraising and alumni or donor engagement efforts at non-profits and universities worldwide, about a wide-reaching data security incident impacting Inova and many of Blackbaud's clients across the world. Blackbaud was the target of a ransomware attack that occurred between February 7, 2020 and May 20, 2020. As a result of this incident, hackers obtained some of the personal information of Inova's patients and donors.

On August 10, 2020, Inova determined that the information removed by the threat actor may have contained a limited amount of personal information, including full names, addresses, dates of birth, phone numbers, provider name(s), date(s) of service, and/or hospital department(s). Philanthropic giving history, such as donation dates and amounts, may have also been removed by the threat actor. This incident does not impact Social Security numbers and financial account information and/or payment card information were also not exposed. The Inova electronic health record system was not impacted by this incident.

According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity. Also according to Blackbaud, they paid the threat actor to ensure that the data was

permanently destroyed. Nevertheless, out of an abundance of caution, Inova 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. Inova is providing the affected residents with written notification of this incident commencing on or about September 9, 2020 in substantially the same form as the letter attached hereto. Inova 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. The affected residents are also being provided steps to take to safeguard themselves against medical identity theft.

At Inova, protecting the privacy of personal information is a top priority. Inova remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Blackbaud has assured Inova that they closed the vulnerability that allowed the incident to occur and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. Inova will continually evaluate and modify its practices, and those of its third-party service providers, to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

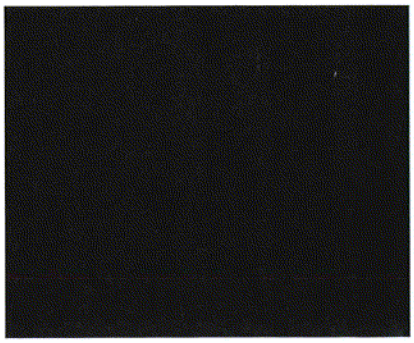
Sincerely,

Dominic A. Paluzzi

Encl.

INOVA

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



IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Inova Health System ("Inova"). We are writing with important information regarding a recent data security incident at Blackbaud, a third party service provider, which may have involved some of the information that you provided to Inova. Blackbaud is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at non-profits and universities worldwide. Inova uses one or more Blackbaud applications, and Blackbaud recently experienced an incident impacting information held on one of those applications. We want to provide you with information about the incident and the significant measures we are taking to protect your information.

What Happened

On July 16, 2020, Blackbaud notified Inova of a wide-reaching security incident that impacted Blackbaud's clients across the world. Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed us that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020. According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed.

What Information Was Involved

On August 10, 2020 we determined that the information removed by the threat actor may have contained some of your personal information, including your full name, address, date of birth, phone number, provider name(s), date(s) of service, and/or hospital department(s). Your philanthropic giving history, such as donation dates and amounts, may have also been removed by the threat actor. **This incident does not impact your Social Security number, which we do not collect, and your financial account information and/or payment card information were also not exposed. The Inova electronic health record system was not impacted by this incident.**

What We Are Doing

Upon learning of the issue, we commenced an immediate and thorough investigation. That investigation is still ongoing. As part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged cybersecurity professionals experienced in handling these types of incidents.

What Blackbaud is Doing

Blackbaud has assured us that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. **According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity**. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What You Can Do

This letter provides precautionary measures that 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. We have also included information on protecting your medical information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

For More Information

Please know the security of our patients' and donors' information is our top priority, and we deeply apologize for any inconvenience this may cause. We remain fully 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 those of our third party service providers, to enhance the security and privacy of your personal information.

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 protect your information. The response line is available Monday through Friday, 9 am to 9 pm Eastern Time.

Sincerely,

[redacted]

Inova Health System

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one (1) 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. 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
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO 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, youmay obtain information from the FTC about fraud alerts and security freezes.

NOTE: The above-referenced protections *may* not be available to minor children or those without credit files. If this notice letter is addressed to a minor child or an individual without a credit file, we recommend that you contact the consumer reporting agencies to determine what steps, if any, you should take to safeguard the addressee's information.

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.

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.