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

July 28, 2020

VIA U.S. MAIL

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

Re: Beaumont Health – Incident Notification

Dear Sir or Madam:

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

Beaumont was the target of an email phishing campaign that resulted in an unauthorized individual gaining access to the email accounts of a small number of employees. Upon learning of the issue, Beaumont commenced a prompt and thorough investigation, working closely with external cybersecurity professionals. After an extensive forensic investigation and comprehensive manual document review, Beaumont discovered on June 5, 2020 that one or more of the email accounts that were accessed between January 3, 2020 and January 29, 2020 contained some of the resident's personal and protected health information. One or more of the email accounts contained the following information about the resident: medical diagnosis, date you received medical care, and your age

Beaumont has no indication that any information has been misused. Nevertheless, out of an abundance of caution, Beaumont 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. Beaumont will provide the affected resident with written notification of this incident commencing on or about July 28, 2020 in substantially the same form as the letter attached hereto. The affected resident is being provided with advice on steps he or she can take to prevent medical identity theft.

At Beaumont, protecting the privacy of personal information is a top priority. Beaumont has taken significant measures to prevent this from happening again, including improving its multi-factor authentication software, conducting an enterprise-wide risk analysis, and retraining

its workforce on identifying and responding to phishing attacks. Beaumont is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Beaumont will continue to evaluate and modify its practices and internal controls to enhance the security and privacy of personal information.

Notice is being provided pursuant to the HIPAA Breach Notification Rule, 45 CFR §§ 164.400, *et seq.*

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

Sincerely,

James J. Giszczak

Encl.

Beaumont

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULY

[redacted]

[redacted]

Dear [redacted],

The privacy and security of the personal information we maintain is of the utmost importance to Beaumont Health ("Beaumont"). We are writing to inform you of a recent data security incident that we identified and addressed that may have involved some of your information. This letter provides information about the incident, explains the services we are providing to you, and explains how we protect your information.

What Happened?

Beaumont was the target of an email phishing campaign that resulted in a limited number of employees receiving a suspicious email containing a malicious link. A small number of employees fell victim to the phishing campaign, resulting in an unauthorized individual gaining access to those employees' email accounts. Upon learning of the incident, Beaumont disabled the accessed email accounts and required mandatory password resets to prevent further misuse.

There is no evidence that the purpose of the phishing campaign was to obtain patient information and we have no evidence that any information was actually acquired or used by the unauthorized individual. However, we are providing notice out of an abundance of caution.

What We Are Doing.

Upon learning of this issue, we commenced a prompt and thorough investigation, working closely with external cybersecurity professionals. After an extensive forensic investigation and comprehensive manual document review, we discovered on June 5, 2020 that one or more of the email accounts that were accessed between January 3, 2020 and January 29, 2020 contained some of your personal and/or protected health information.

We are currently in the process of implementing additional technical safeguards on our email system to prevent the recurrence of similar incidents. We have also implemented additional training and education for our employees to increase awareness of the risks of malicious emails and to educate employees on identification and handling of malicious emails.

What Information Was Involved.

One or more of the accessed email account(s) contained some of your personal and/or protected health information, including [redacted].

What You Can Do.

We have no evidence that any of your information has been acquired or misused. However, we recommend that all patients and personal representatives of patients monitor insurance statements for any transactions related to care or services that have not actually been received. We are also including a list of steps that can be taken to help protect your medical information.

For More Information.

Please accept our sincere apologies that this incident occurred. We have taken significant measures to prevent this from happening again, including improving our multi-factor authentication software, conducting an enterprise-wide risk analysis, and retraining our workforce on identifying and responding to phishing attacks. We remain fully committed to maintaining the privacy of all personal information in our possession. We continually evaluate and modify our practices to enhance the security and privacy of your personal information and are committed to implementing additional safeguards to prevent recurrence of future 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 about what you can do to help protect your information. The response line is available Monday through Friday, 9:00 a.m. to 6:30 p.m. EST.

Sincerely,

[redacted]
Beaumont Health

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.

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.