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

Colin M. Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

March 11, 2022

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Labette Health – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents Labette Health. I am writing to provide notification of an incident at Labette Health that may affect the security of personal information of approximately eight (8) New Hampshire residents. Labette Health'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, Labette Health does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On October 14, 2021, Labette Health discovered potential unauthorized access to its network. Upon learning of this issue, Labette Health immediately took steps to secure its network and mitigate against any additional harm. Labette Health also immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine whether any sensitive data had been compromised as a result of the incident. Labette Health's investigation determined that the unauthorized individual(s) potentially accessed and acquired information from portions of its network between October 15, 2021 and October 24, 2021. On February 11, 2022, following an extensive review and analysis of the data at issue, Labette Health determined that certain files and folders that may have been accessed or acquired in this incident contained the New Hampshire residents' full name and one or more of the following (to the extent it resided on Labette Health's system): Social Security number, medical treatment and diagnosis information, treatment costs, dates of service, prescription information, Medicare or Medicaid number, and/or health insurance information.

Labette Health is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Labette Health 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. Labette Health is providing the affected residents with written notification of this incident commencing on or about March 11, 2022 in substantially the same form as the letter attached hereto. Labette Health is offering the affected residents complimentary one-year membership with a credit monitoring service. Labette Health will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Labette Health will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files, obtaining free credit reports, and practices and safeguards to protect against

medical theft. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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. Labette Health is 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.

At Labette Health, protecting the privacy of personal information is a top priority. Labette Health is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. In response to this incident, Labette Health has strengthened its network and implemented additional security improvements recommended by third-party cyber security experts. These include resetting account passwords and strengthening its password security policies, implementing multi-factor authentication for network access, upgrading its endpoint detection software, and coordinating additional employee training related to network security and threat detection.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,

Colin M. Battersby

Encl.

Labette Health
We Center Around You.

[redacted]

To Enroll, Please Call:
1-833-774-1216
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [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 Labette Health. 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.

On October 14, 2021, Labette Health identified unauthorized access to our network. Upon learning of the issue, we immediately took steps to secure our network and mitigate against any additional harm. Additionally, we launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine whether any sensitive data had been compromised as a result. After an extensive forensic investigation we determined that as part of this incident, an unauthorized individual accessed and acquired information from our network between October 15, 2021 and October 24, 2021. Following a thorough review of the files that were removed, we discovered on February 11, 2022 that your full name and one or more of the following (to the extent it resided on our system) may have been accessed or acquired in this incident: Social Security number, medical treatment and diagnosis information, treatment costs, dates of service, prescription information, Medicare or Medicaid number, and/or health insurance information.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of identity theft protection services through IDX, which includes 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

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 included suggestions for protecting your medical 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. In response to this incident, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts. These include resetting account passwords and strengthening our password security policies, implementing multi-factor authentication for network access, upgrading our endpoint detection software, and coordinating additional employee training related to network security and threat detection.

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 against misuse of your information. The response line is available Monday through Friday, **8 a.m. to 8 p.m. Central Time.**

Sincerely,

Labette Health

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **IDX website** to enroll: https://app.idx.us/account-creation/protect
3. PROVIDE the **Enrollment Code**: [redacted]

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at 1-833-774-1216.

2. **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
(800) 525-6285
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
P.O. Box 105788
Atlanta, GA 30348

Experian
(888) 397-3742
https://www.experian.com/fraud/center.html
P.O. Box 9554
Allen, TX 75013

TransUnion LLC
(800) 680-7289
https://www.transunion.com/fraud-alerts
P.O. Box 6790
Fullerton, PA 92834-6790

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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

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

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/credit-freeze
(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.

If this notice letter states that your financial account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

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.