

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

February 12, 2024

VIA EMAIL: Idtheft@oag.state.md.us

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Lexington Health, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Lexington Health, Inc. (d/b/a Lexington Medical Center and hereinafter “LMC”) of West Columbia, South Carolina. I am writing to provide notification of an incident at LMC that may affect the security of personal information of approximately two (2) Maryland residents. By providing this notice, LMC does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction. Notice is being provided under the Health Insurance Portability and Accountability Act Breach Notification Rule, 45 C.F.R. §§ 164.400-414 (“HIPAA” or “Final Rule”).

On October 4, 2023, an unauthorized party accessed one (1) LMC employee email account and the employee’s individual data drive. Upon detecting the unauthorized activity, LMC immediately contained the incident and commenced an immediate and thorough investigation. As part of its investigation, LMC engaged leading cybersecurity experts to identify what personal information, if any, was involved.

After an extensive forensic investigation and manual document review, LMC discovered on or about January 18, 2024 that a limited number of the files contained in the employee email account and/or the employee’s associated individual data drive contained billing-related documents with personal information pertaining to a limited number of Maryland residents, such as full names, dates of birth, medical record numbers, health insurance identification numbers, patient charge descriptor information, and billing codes. The elements of information varied per individual.

To date, LMC is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, LMC 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. LMC is providing the affected residents with written notification of this incident commencing on or about February 12,

February 12, 2024

Page 2

2024 in substantially the same form as the letter attached hereto. LMC 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 LMC, protecting the privacy of personal information is a top priority. LMC is committed to maintaining the privacy of personal information in its possession and has taken many precaution to safeguard it. LMC continually evaluates and modifies its practices and internal controls 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.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]:

We are writing to inform you of a data security incident at Lexington Medical Center involving some of your information. We wanted 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 October 4, 2023, an unauthorized party accessed one (1) employee email account and the employee's individual data drive.

What We Are Doing

Upon detecting the unauthorized activity, we immediately contained the incident and commenced an immediate and thorough investigation. As part of our investigation, we engaged leading cybersecurity experts to identify what personal information, if any, was involved.

What Information Was Involved?

After an extensive forensic investigation and manual document review, we discovered on or about January 18, 2024 that a limited number of the files contained in the employee email account and/or the employee's associated individual data drive contained billing-related documents that may have included your full name, date of birth, medical record number, health insurance identification number, patient charge descriptor information, and billing codes. There is no way to determine with certainty whether the unauthorized party accessed these specific files, however, out of abundance of caution, we want to make you aware. Please be assured that your Social Security number and electronic medical record were **not** accessed as a result of this matter.

What You Can Do.

We have no evidence that any personal information has been or will be misused as a direct result of this incident. This letter provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and 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 are also suggesting steps you can take to protect 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 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, 9:00am-9:00pm EST.

Sincerely,

Lexington Medical Center

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

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 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

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

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

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

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://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.

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. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against 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.

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.

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, <https://www.marylandattorneygeneral.gov/>, Telephone: 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: 1-877-566-7226.