BakerHostetler

Baker&Hostetler LLP
2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891
T 215.568.3100
F 215.568.3439
www.bakerlaw.com
Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

March 26, 2021

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

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Lexington Medical Center ("LMC") (formerly known as Lexington Memorial Hospital), a non-profit medical facility located in Lexington, North Carolina, regarding a security incident that occurred at LMC's former vendor, Healthgrades Operating Company, Inc. ("Healthgrades"). LMC is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

On January 29, 2021, LMC received notification about a data privacy incident from Healthgrades, a vendor LMC formerly used for educating patients and the Lexington community about LMC's services and health matters. Healthgrades advised that an unauthorized individual had gained access to a Healthgrades archived server between October 16, 2020 and October 28, 2020. Healthgrades discovered that the archived server involved in the incident contained backup files with LMC patient information from the time it provided services to LMC. The files included information from mid-2010 to mid-2011. After receiving notification, LMC immediately took steps to understand the extent of the incident and the data involved.

LMC's investigation and review of the backup files involved in the incident determined that they contained information belonging to two (2) LMC patients who are New Hampshire residents. The information involved for the residents includes names, addresses and Social Security numbers. This incident was limited to the Healthgrades systems only and did not involve any access to LMC's systems or electronic health records.

LMC began mailing letters to the New Hampshire residents on March 26, 2021 in accordance with HIPAA and N.H. Rev. Stat. Ann. § 359-C:20.[1] LMC is also offering the notified residents one year of complimentary identity monitoring services through Kroll. A copy of the notification letter is enclosed. To help prevent something like this from happening again, LMC obtained assurances from Healthgrades that no LMC patient data remains on their systems. LMC has similarly reviewed its files and confirmed that no patient information is being sent to Healthgrades.

Sincerely,

Eric A. Packel
Partner

Enclosure

[1] This report is not, and does not constitute, a waiver of LMC's objection that New Hampshire lacks personal jurisdiction over LMC regarding any claims related to this data security incident.

Lexington Medical Center

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Su información personal puede haber estado involucrada en un posible incidente cibernético. Si desea recibir una versión de esta carta en español, por favor llame 1-855-660-1531.

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Lexington Medical Center (LMC) (formerly known as Lexington Memorial Hospital) is proud to provide quality healthcare for our community, and we are honored by the trust you and others place in us to care for you. We recognize an important part of that trust includes protecting the privacy and security of your information, including when that information is maintained by our vendors. Unfortunately, we have discovered that Healthgrades Operating Company, Inc. ("Healthgrades"), a vendor who previously provided services to LMC, has had a security incident that involved some of your information.

What Happened?

Healthgrades previously assisted LMC in educating patients and the community about health matters and available services at LMC. In order to provide those services, Healthgrades was provided some LMC information. On January 29, 2021, Healthgrades notified us that an unauthorized individual gained access to a Healthgrades archived server between October 16, 2020 and October 28, 2020. Healthgrades discovered that the impacted archived server included backup files with LMC patient information from the time it provided services to LMC. The files included information from mid-2010 to mid-2011.

What Information Was Involved?

As soon as we were notified by Healthgrades, we immediately took steps to understand the circumstances of the incident and the information impacted. We understand that the Healthgrades files involved in the incident were archived files maintained by Healthgrades from the time when they provided services to LMC. The information in the files did not include your financial account information. In addition, because LMC is no longer using Healthgrades to provide these services, the files did not include information from any recent services.

The archived files may have included your name, address, demographic and contact information, Social Security number, date of birth, LMC medical record number, date(s) of service, patient type, limited health information such as treatment and billing codes and their descriptions (which, in some cases, may indicate a diagnosis), physician names, physician specialty, guarantor name, insurance type, insurance provider, and/or cost of treatment information. This incident was limited to the Healthgrades systems only and did **not** involve any LMC systems or electronic health records.

What Are We Doing in Response?

We care about the privacy and security of our patients' information and take this matter very seriously. To help prevent something like this from happening again, we have obtained assurances from Healthgrades that no LMC patient data remains on their systems. LMC has similarly reviewed its files and confirmed that no patient information is being sent to Healthgrades. Finally, Healthgrades has also advised us that they have notified law enforcement of this incident and will cooperate with any follow up investigation.

What Can You Do?

Although we have received no indication that your information has been misused, out of an abundance of caution, we are offering you complimentary identity monitoring services through Kroll for one year. The services being offered

include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. We also recommend you review the statements you receive from your healthcare providers. If you see services you did not receive, please contact the provider immediately. **For more information about the identity monitoring services, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the pages that follow this letter.**

For More Information

We are very sorry for any concern or inconvenience this incident may cause you. If you have questions, please contact 1-855-660-1531, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,

Patricia Corn

Chief Privacy Officer

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by **June 23, 3021**. Your Membership Number will not work after this date.
2. Visit **https://enroll.idheadquarters.com** to activate your identity monitoring services.
3. Provide Your Membership Number: **<<Member ID>>**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Lexington Medical Center's mailing address is 250 Hospital Drive, Lexington NC 27292 and the phone number is 336-238-4557.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov