CMC
CATHOLIC MEDICAL CENTER

April 22, 2024

Via U.S. Mail

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capital Street
Concord, NH 03301

RE: Catholic Medical Center – Notice of Vendor Data Security Incident

To Whom It May Concern:

Pursuant to NH RSA 359-C:20, I am writing to report a security incident on behalf of Catholic Medical Center ("CMC") relating to one of our vendors, Lamont Hanley & Associates ("LH"). LH provides account receivable management services to CMC.

On March 6, 2024, LH notified CMC that it discovered that one LH employee email account (the "Compromised Account") was accessed by an unauthorized party via a phishing attempt. Upon detecting the incident, LH commenced an immediate and thorough investigation, contained and secured the email environment, and changed the password to the Compromised Account. As part of the investigation, LH engaged external cybersecurity professionals to investigate the extent of the incident and what, if any, sensitive data, including personal and/or health information may have been accessed and/or acquired by the unauthorized party. The investigation did not identify evidence of specific data access or acquisition by an unauthorized party, but could not conclude with one-hundred percent certainty that data within the account was not accessed or acquired by an unauthorized party. Therefore, out of an abundance of caution, LH conducted an extensive review of the Compromised Account to determine what data may have been involved.

After a thorough forensic investigation and comprehensive manual review of all emails and attachments within the Compromised Account, on February 28, 2024, LH determined individual personal information was present within the Compromised Account. LH immediately notified affected business partners about the incident, including CMC, who has a total of 2,792 patients affected, the vast majority of whom are NH residents. The information involved includes individual

LH has reported no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, CMC is informing you (and the affected individuals) of the incident. LH has been collaborating with CMC to notify all affected individuals and offer complimentary membership with a credit monitoring service if their social security number was involved. Written notification to individuals of this incident with more information about how they can protect themselves against identity fraud will commence this week in substantially the same form as the letter attached hereto.

Patient privacy and security are of the highest importance to CMC. Although CMC's network was not breached as a result of this incident, we maintain an aggressive cyber security program. We also require our contracted vendors to implement administrative, technical, and physical safeguards to secure all sensitive information within their organization.

If you have any questions or need additional information, please contact me at

Sincerely,

Jessica Arvanitis
Compliance & Privacy Officer

Encl.

Cc: Jason Cole, Vice President & General Counsel

[NAME AND ADDRESS]

DATE

Dear NAME

Lamont Hanley & Associates, Inc. ("LH") writes to inform you of a potential data security incident that may involve some of your individual personal and/or health information. LH is a company specializing in accounts receivable management solutions. We were contracted by Catholic Medical Center to provide accounts receivable services on their behalf. 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 personal and/or health information.

What Happened?

On June 20, 2023, LH discovered one employee email account (the "Compromised Account") was accessed by an unauthorized party.

What We Are Doing.

Upon detecting the incident, LH commenced an immediate and thorough investigation, contained and secured the email environment, and changed the password to the Compromised Account. As part of the investigation, LH engaged external cybersecurity professionals to investigate the extent of the incident and what, if any, sensitive data, including personal and/or health information may have been accessed and/or acquired by the unauthorized party. The investigation did not identify evidence of specific data access or acquisition by an unauthorized party but could not conclude with one-hundred percent certainty that data within the account was not accessed or acquired by an unauthorized party. Therefore, out of an abundance of caution, we conducted an extensive review of Compromised Account to determine what data may have been involved.

After a thorough forensic investigation and comprehensive manual review of all data within the Compromised Account, on February 28, 2024, we determined your personal information was present within the Compromised Account. We immediately notified Catholic Medical Center and its Compliance & Privacy Officer, Jessica Arvanitis, and worked with her to notify you of this incident.

What Information Was Involved?

The information potentially involved includes your

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your personal and/or health information as a direct result of this incident. Nevertheless, out of an abundance of caution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 1 Yearfrom the

date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. **Please see enrollment instructions on the next page**.

This letter also provides 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 in the "Other Important Information" section.

For More Information.

LHA values your privacy and deeply regrets 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. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

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 1-833-792-8144. 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, 8am – 8pm. Eastern Time, excluding holidays.

Sincerely,

Lamont Hanley & Associates, Inc.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

To enroll in Credit Monitoring services at no charge, please log on to <<URL>> and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>.** In order for you to receive the monitoring services described above, you must enroll within from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 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
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

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/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
1-888-909-8872

In order to place the security freeze, you will 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. Protecting Your Medical Information.

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.

6. 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.

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.

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 (Toll-free within North Carolina), 919-716-6000.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.