MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 27, 2023

VIA U.S. MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Howard Memorial Hospital ("HMH") located at 130 Medical Circle, Nashville, Arkansas 71852, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. By providing this notice, HMH does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 4, 2022, HMH became aware of suspicious activity within its computer network, and allegations made by an unknown actor that data had been stolen from the HMH network. Steps were promptly taken to secure HMH's network, and an investigation began with assistance from outside cybersecurity specialists to determine the nature and scope of this activity and to safely maintain full operational functionality so HMH could continue to treat patients. HMH learned that certain files were potentially stolen from its network by an unknown actor between November 14 - December 4, 2022.

HMH worked diligently to perform a comprehensive review of at-risk files in order to identify individuals whose information may have been impacted by this event. Ultimately, HMH made the decision to notify all current or former patients and employees, in an abundance of caution, due to a potential impact to their information. Therefore, HMH provided notification to those current or former employees and patients whose information was present on HMH systems at the time of the data security event and was therefore potentially impacted by the event.

The information that could have been subject to unauthorized access includes name, contact information, date of birth, Social Security number, health insurance information, medical record number (MRN), medical history, diagnosis, treatment information, and physician name.

Notice to New Hampshire Residents

On or about January 27, 2023, HMH provided written notice of this incident to approximately two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Prior to mailing written notifications, HMH also posted notification on its website, and provided notification to media in Arkansas, on December 29, 2022.

Other Steps Taken and To Be Taken

Upon discovering the event, HMH moved quickly to investigate and respond to the incident, assess the security of HMH systems, and identify potentially affected individuals. Further, HMH notified federal law enforcement regarding the event. HMH is also working to implement additional safeguards and training to its employees. HMH is providing access to credit monitoring services for one (1) year through Sontiq, a Transunion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HMH is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HMH is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

HMH is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. HMH is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at

Very truly yours,

Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/jrm
Enclosure

EXHIBIT A

Howard Memorial Hospital
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

January 27, 2023

NOTICE OF SECURITY INCIDENT

Dear [redacted]:

Howard Memorial Hospital ("HMH") is writing to provide you with notice of a recent data security event that may impact the confidentiality and security of some of your information. We are providing you with information about the event, our response, and steps you can take to better protect your information against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On December 4, 2022, HMH became aware of suspicious activity within its computer network, and allegations made by an unknown actor that data had been stolen from the HMH network. Steps were promptly taken to secure HMH's network, and an investigation began with assistance from outside cybersecurity specialists to determine the nature and scope of this activity and to safely maintain full operational functionality so HMH could continue to treat patients. HMH learned that certain files were potentially stolen from its network by an unknown actor between November 14 - December 4, 2022.

HMH worked diligently to perform a comprehensive review of at-risk files in order to identify individuals whose information may have been impacted by this event. Ultimately, HMH made the decision to notify all current or former patients and employees, in an abundance of caution, due to a potential impact to their information. Therefore, HMH is providing you with this notification given that your information was present on HMH systems at the time of the data security event and was therefore potentially impacted by this event.

What Information Was Involved? Our investigation determined that the types of information potentially impacted for patients, including you, includes name, contact information, date of birth, Social Security number, health insurance information, medical record number (MRN), medical history, diagnosis, treatment information, and physician name.

What We Are Doing. HMH takes this event and the security of patient information in our care very seriously. Upon learning of this event, we immediately took steps to secure our network and ensure that we could maintain operations in a safe and secure fashion. As part of our ongoing commitment to data privacy, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on our systems. Notice was also provided to federal law enforcement and will be provided to the U.S. Department of Health and Human Services.

As an added precaution, we are offering you 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 12 months from 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. If you wish to activate the credit monitoring services, you may follow the instructions included in the *Steps You Can Take to Protect Your Personal Information.*

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Your Personal Information* which contains information on what you can do to better safeguard against possible misuse of your information. You can also enroll to receive the complimentary credit monitoring and identity protection services through Sontiq, a TransUnion company. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-833-570-2728, 7:00 AM – 7:00 PM Central, Monday through Friday, excluding holidays.

Sincerely,

Howard Memorial Hospital

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/howardmemorial** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us: You may obtain information from these sources and/or the Federal Trade Commission using the contact information noted above about steps you can take to avoid identity theft. Howard Memorial Hospital is located at 130 Medical Circle, Nashville, Arkansas 71852.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.