WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

September 30, 2025

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

<u>Via Online Portal:</u>

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Cybersecurity Incident Involving Shelby County Chris A. Myrtue Memorial Hospital, dba Myrtue Medical Center

Dear Attorney General Hilgers:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Shelby County Chris A. Myrtue Memorial Hospital, dba Myrtue Medical Center ("MMC"), a healthcare services provider located in 1213 Garfield Ave., Harlan, IA 51537, with respect to a recent cybersecurity incident that was first discovered by MMC on June 13, 2025 (hereinafter, the "Incident"). MMC takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter is an update to the incident notice submitted to your office on July 21, 2025. This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Nebraska residents being notified, and the steps that MMC has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services. MMC is still in the midst of the investigation. We will provide an update regarding the incident when the investigation is completed.

1. Nature of the Incident

On June 13, 2025, MMC discovered the Incident when MMC detected unusual activity on its computer network. Upon discovery of the incident, MMC promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. While the forensic investigation is still ongoing, MMC is providing notice to all former employees whose information may have been impacted and the former employee's dependents in the abundance of caution. MMC immediately began a thorough review of the potentially accessed files to identify the individuals whose sensitive information was present at the time of the incident. This step is necessary so that MMC may send a notice of the Incident to the potentially impacted clients.

Although MMC is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, and social security number may have been exposed as a result of this unauthorized activity.

As of this writing, MMC has not received any reports of related identity theft since the date of the incident (June 13, 2025 to present).

2. Number of Nebraska residents affected.

A total of fifty (50) Nebraska residents may have been potentially affected by this incident. Notification letters to ten (10) Nebraska residents were mailed on July 21, 2025, by U.S. First Class Mail. Notification letters to the additional impacted individuals by the incident are being mailed on September 30, 2025, by U.S. First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

MMC is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MMC moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, MMC engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MMC disconnected all remote access to its network, changed administrative credentials, enhanced the security measures, and took steps and will continue to take steps to mitigate the risk of future harm. Lastly, MMC informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although MMC is not aware of any actual or attempted misuse of the affected personal information, MMC offered 12 months of complimentary credit monitoring and identity theft restoration services through TransUnion to all individuals to help protect their identity. Additionally, MMC provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

MMC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Shelby County Chris A. Myrtue Memorial Hospital
dba Myrtue Medical Center
c/o Cyberscout
PO Box 1286 Dearborn, MI 48120-9998

VIA FIRST-CLASS MAIL

[redacted]

000010102G0400 P

September 30, 2025

Notice of Data Security Incident

Dear [redacted]

This letter is to inform you that Shelby County Chris A. Myrtue Memorial Hospital, dba Myrtue Medical Center ("MMC") was recently subject to a data security incident that may have resulted in unauthorized access to your personal information. With this notice we are providing you with details about the incident, steps we are taking in response to the incident, and resources available to help you protect against the potential misuse of your information.

What Happened?

On June 13, 2025, MMC detected unusual activity on its computer network (the "Incident"). Upon discovery of the Incident, MMC immediately disconnected access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the Incident. While the forensic investigation is ongoing, the preliminary findings indicate that some MMC files were accessed by an unauthorized actor.

Based on the preliminary findings, MMC has begun a lengthy and comprehensive review of our systems to determine the scope of the access. While the review remains ongoing, we have identified that some of your personal information may have been impacted by the Incident. As part of the ongoing process, MMC is notifying you of the Incident in that you may take the appropriate precautionary steps to secure your information.

What Information Was Involved?

The information potentially impacted will vary by individual. At this time, it appears that certain information related to you may have been subject to unauthorized access. The type of personal information may include one or more of the following data elements: name, driver's license number or identification number, social security number, and direct deposit information.

What We Are Doing

Data privacy and security is among MMC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the Incident, MMC moved quickly to investigate, respond, and confirm the security of its computer systems. Specifically, MMC disconnected remote access to its network, changed administrative credentials, enhanced the security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

In light of the Incident, 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 twelve (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 TransUnion specializing in fraud assistance and remediation services.

<u>What You Can Do</u>

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate 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 ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (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.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at www.ftc.gov/idtheft.

We 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 or unauthorized activity. Any taxpayer can proactively request an Identity Protection PIN (IP PIN) to ensure no one else files their return without authorization. Instructions for obtaining an IP PIN are available at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If a taxpayer suspects fraudulent activity, such as a return submitted without their authorization, they should complete IRS Form 14309 Identity Theft Affidavit at https://www.irs.gov/dmaf/form/f14039.

Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

We encourage all employees to take advantage of these services.

<u>For More Information</u>

MMC recognizes that you may have questions not addressed in this letter. If you have additional questions, please call 1-800-405-6108 (toll free) during the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday (excluding U.S. national holidays).

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you.

Sincerely,

SHELBY COUNTY CHRIS A. MYRTUE MEMORIAL HOSPITAL,
DBA MYRTUE MEDICAL CENTER

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

P 0000102028000

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General’s office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.