October 13, 2026

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

Via E-Mail:
Attorney General Brenna Bird
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notice of Cybersecurity Incident Involving Shelby County Myrtue Medical Center

Dear Attorney General Bird:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Shelby County Myrtue Medical Center ("MMC") (located at 1213 Garfield Ave, Harlan, IA51537). The purpose of this correspondence is to provide your office with notice of a 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 will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Iowa residents being notified, and the steps MMC has taken in response to the Incident. We have also attached a sample of the notification made to potentially impacted individuals.

1. Nature of the Incident

On June 13, 2025, MMC detected suspicious activity on their network that resulted in a network interruption. MMC immediately isolated the impacted environment and worked with its IT professionals and outside experts to secure and remediate the server. MMC engaged a third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The investigation determined that an unauthorized third-party potentially viewed and/or downloaded data stored on certain of the MMC's systems.

Based on these findings, MMC conducted an extensive review of the impacted data files to identify the specific individuals and the types of information that may have been compromised. Due to the size of the potentially impacted population, MMC provided substitute notice through a website posting and media notice on June 27, 2025, while engaging a third-party vendor to identify potentially impacted individuals and information involved. Following completion of that review and subsequent address verification the notice population was established on August 24, 2026. On October 8, 2026, MMC finalized the list of individuals to notify. The type of information that may have been compromised includes Driver's License Number, Credit Card Number in combination with Access Code, Social Security Number, and Name.

2. Number of Iowa residents affected.

A total of three thousand seven hundred and fourteen (3,714) Iowa residents require notice because their personal information—as defined by Iowa law may have been affected. Notification letters to these individuals were mailed on October 13, 2026, by U.S. mail. A sample (redacted) copy of the notification letter is included with this letter as **Exhibit A**.

3. Steps taken in response to the Incident.

Data privacy and security are among one of MMC's highest priorities, and MMC is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the Incident, MMC immediately isolated the impacted systems and worked with IT professionals and outside experts to secure and remediate these systems. MMC engaged a third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the Incident. Furthermore, MMC is implementing additional technical safeguards, enhanced security measures, and updated policies and procedures to mitigate against the risk of future issues.

MMC has highlighted steps that individuals can take to protect themselves including actively monitoring their financial accounts and statements, requesting a free credit report, and placing a fraud alert or security freeze on their credit reports.

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 the undersigned at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

Anjali C. Das

343633828v.1

EXHIBIT A

343633828v.1

Shelby County Chris A. Myrtue Medical Center
d/b/a Myrtue Medical Center
PO Box 1286
Dearborn, MI 48120-9998

Logo

Jane A Smith Jr
123 Main St
Apt A
Sample, XX ABC12 DE34

Date

Draft

Re: Notice of TEST

Dear Jane Smith,

Shelby County Myrtue Medical Center ("MMC") is writing to inform you of an event that may have involved unauthorized access to certain personal information ("PI") and/or protected healthcare information ("PHI") related to you. MMC has records in our possession containing some of your PI and PHI because you were a current or former patient of MMC. We take the protection of your PI and PHI very seriously and are sending you this notice to tell you what happened, what information was involved, and what we have done in response. Additionally, this letter will tell you what you can do in response to this incident and what resources are available to help protect against the potential misuse of PI and/or PHI, if you feel it is appropriate.

What Happened?

On or about June 13, 2025, MMC became aware of suspicious activity within our network environment. We immediately took steps to lock down and secure our environment and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the activity. On July 17, 2025, the forensic investigation concluded. It confirmed that data had been taken from its systems without authorization and identified the affected data from the compromised systems.

We engaged a third-party vendor to data mine the data identified by the forensics investigation. The third-party vendor reviewed the affected data to identify the types of information that may have been compromised and the individuals potentially affected by this incident. The data mining vendor completed its review on June 5, 2026. Following the third-party data-mining review, we undertook detailed internal review of our records to identify contact information to provide notifications.

The list of individuals to notify was finalized on <<post-NCOA date>>, followed by organizing the mailing, call center, and credit monitoring services for the impacted population. This process was necessary to accurately identify whose PI and PHI may have been affected and provide notice to the potentially impacted individuals. During this review, we determined that some of your PI and/or PHI may have been affected by the incident.

What Information Was Involved?

The PI and/or PHI that may have been subject to unauthorized access includes: Name, Demographic Information, Social Security Number, Government Identifiers, Health or Medical Information, Account Credentials, Health Insurance Information, or Financial Account Information. Please note the information impacted varies for each potentially impacted individual.

What We Are Doing.

MMC takes this event and the security of information in our care very seriously. Upon discovery of this event, we promptly commenced an investigation and assessed the security of its systems with the assistance of outside experts. While our investigation was ongoing, we proactively began notifying potentially impacted individuals via our website and through notice to the media notice on June 27, 2025. In addition, we have taken additional technical and administrative steps to further enhance the security of our systems and customer data to mitigate the risk of future harm.

In response to the incident, we are offering <<Service Length>> months of 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 <<Service Length>> 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 the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

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: **ABC123DEF456**. 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.

What You Can Do.

As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. We encourage you to enroll in the complimentary credit monitoring that we are offering to you at no cost. Additional information can be found in Additional Resources to Help Protect Your Information.

For More Information.

If you have any questions or concerns not addressed in this letter, please call our dedicated line 1-844-507-8924 (toll free) Monday through Friday, during the hours of 8 a.m. and 8 p.m. Eastern Time (excluding U.S. national holidays).

We sincerely regret any concern or inconvenience this matter may cause and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Shelby County Myrtue Medical Center

Draft

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.

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. Please contact Myrtue Memorial Center at 1213 Garfield Ave, Harlan, IA 51537 or by phone, 712-755-5161.

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. There were # residents of Rhode Island potentially impacted by this incident.