[redacted]

McAlester Regional Health Center
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Exhibit A

[redacted]

November 15, 2023

Notice of Data Security Incident

Dear [redacted],

McAlester Regional Health Center is writing to inform you of an incident that may have impacted your personal information described in more detail below. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On May 8, 2023, McAlester Regional Health Center detected suspicious activity that impacted access to some of its systems. As soon as McAlester Regional Health Center learned about this activity, it immediately implemented its incident response protocols, disconnected all systems, and engaged external cybersecurity experts to conduct a forensic investigation. The investigation found that there had been unauthorized access to some information stored on McAlester Regional Health Center's systems. Out of an abundance of caution, a vendor was engaged to review the impacted data to identify any personal information found there and to whom it belonged. This process was completed on October 23, 2023, at which point McAlester Regional Health Center determined that your personal information may have been present during the period of unauthorized access.

What Information Was Involved?

Impacted information may include some combination of your name, address, and Social Security number, driver license or other governmental identification number and date of birth.

What We Are Doing:

McAlester Regional Health Center has taken steps to prevent a similar incident in the future by tightening firewall restrictions, rewriting, and strengthening their password policy, initiating password changes across the organization for every account, and increasing restrictions on the sharing of files.

Although there is no evidence your information has been misused, 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 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.

[redacted]

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/mcalester and follow the instructions provided. When prompted please provide the following unique code to receive services: FQ8XS5LT52 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.

We encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the event and can answer questions or concerns you may have regarding protection of your personal information.

Please monitor your financial statements and credit reports, and immediately report any suspicious activity.

For More Information:

You should contact Cyberscout at the number provided above if you have any questions on protecting your identity or how to enroll in the services provided. If you have any questions or concerns, please call 1-833-602-5714 Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

McAlester Regional Health Center

[redacted]

Recommended Steps to help Protect your Information

1. Activate the credit monitoring provided as part of your services with Cyberscout. The monitoring included must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, Cyberscout will be able to provide guidance.

2. Telephone. Contact Cyberscout at <<number>> to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. Review your credit reports.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in Cyberscout credit monitoring, notify them immediately by calling 1-800-405-6108 from 8:00 am to 8:00 pm Eastern, Monday through Friday.

A representative will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be able to work with a representative who will assist you with resolving any fraudulent activity.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

[redacted]

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 0 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

[redacted]

McAlester Regional Health Center
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

November 15, 2023

Notice of Data Security Incident

Dear Parent or Guardian of [redacted],

McAlester Regional Health Center is writing to inform you of an incident that may have impacted your dependent's personal information described in more detail below. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you and your dependent.

What Happened?

On May 8, 2023, McAlester Regional Health Center detected suspicious activity that impacted access to some of its systems. As soon as McAlester Regional Health Center learned about this activity, it immediately implemented its incident response protocols, disconnected all systems, and engaged external cybersecurity experts to conduct a forensic investigation. The investigation found that there had been unauthorized access to some information stored on McAlester Regional Health Center's systems. Out of an abundance of caution, a vendor was engaged to review the impacted data to identify any personal information found there and to whom it belonged. This process was completed on October 23, 2023, at which point McAlester Regional Health Center determined that your dependent's personal information may have been present during the period of unauthorized access.

What Information Was Involved?

Impacted information may include some combination of your dependent's name, address, and date of birth, medical record number and or patient account number, medical condition or treatment information, medical provider name, individual health insurance policy information and dates of service.

What We Are Doing:

McAlester Regional Health Center has taken steps to prevent a similar incident in the future by tightening firewall restrictions, rewriting, and strengthening their password policy, initiating password changes across the organization for every account, and increasing restrictions on the sharing of files.

Although we have no evidence that your dependent's information will be misused, we are offering access to Cyber Monitoring services for you and your minor child for twelve (12) months at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your

personally identifiable information or your child's is found online. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services

What You Can Do:

While we believe it is unlikely that any of your dependent's information will be misused, we encourage you to enroll in Cyberscout's Cyber Monitoring services. To enroll in Cyber Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/mcalester and follow the instructions provided. When prompted please provide the following unique code to receive services: GK3D26CXDY Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. 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. 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.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. Please call 1- 833-602-5714 and supply the fraud specialist with your unique code listed above. To extend these services, enrollment in the monitoring services described below is required.

Your trust is important to us, and we deeply regret any inconvenience or concern that this incident may cause.

Sincerely,

McAlester Regional Health Center

U.S. State Notification Requirements

For residents of *Hawaii, Michigan, Missouri, New Mexico, Virginia, Vermont, and North Carolina:* It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, Washington, and West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa:* State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Colorado, Maryland, Illinois, North Carolina, and Rhode Island*: You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Attorney General
Consumer Protection Div.
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Attorney General
Consumer Protection Div.
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Attorney General
Consumer Protection Div.
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

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

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of *California*: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

For residents of *District of Columbia*: You may obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia by visiting https://oag.dc.gov/consumer-protection, emailing consumer.protection@dc.gov, calling (202) 442-9828, or mailing Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW Washington, DC 20001.

For residents of *New York*: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

[redacted]

For residents of *Oregon:* You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via each credit bureau's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below. As of September 21, 2018, fraud alerts will now last one year, instead of 90 days. Fraud alerts will continue to be free and identity theft victims can still get extended fraud alerts for seven years.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, each credit reporting agency has a dedicated web page for security freezes and fraud alerts or you can request a freeze by phone or by mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request may also require a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Effective September 21, 2018, placing a freeze on your credit report is now free for all United States citizens

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	http://www.experian.com/freeze	www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.