



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

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

August 23, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Methodist McKinney Hospital (“MMH”) located at 8000 W. Eldorado Parkway, McKinney, Texas 75070, and Methodist Craig Ranch Surgical Center (“MCRSC”) located at 6045 Alma Rd. Suite 100, McKinney, Texas 75070, and the now closed Methodist Allen Surgical Center (“MASC”)¹ formerly located at 125 Raintree Cir. Suite 200, Allen, Texas 75013 and are writing to notify your office of a potential data event that may affect the security of certain personal information relating to one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MMH, MCRSC, and MASC do not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On July 5, 2022, MMH, MCRSC, and MASC became aware of unusual activity on certain systems. MMH, MCRSC, and MASC promptly took steps to better ensure the integrity of the systems and begin an investigation with the assistance of a third-party company. To date the investigation confirmed that an unauthorized actor accessed certain systems containing MMH, MCRSC, and MASC data between May 20, 2022, and July 7, 2022, and copied certain files. Although the investigation is ongoing, as part of the response to this event, MMH, MCRSC, and MASC are conducting a detailed review to determine what information was present in the relevant systems at the time of the unauthorized access and to whom those records relate. MMH, MCRSC, and MASC is also reviewing its records and taking steps to identify address information for purposes of providing individual notice. MMH, MCRSC, and MASC are notifying individuals as information becomes available.

¹ When MASC was closed, MMH assumed ownership of all MASC data.

On or about August 11, 2022, MMH, MCRSC, and MASC completed their most recent review effort and determined that the name, Social Security number, driver's license number, and medical history information of one (1) Maryland resident may have been present in an involved system.

Notice to the Maryland Resident

On or about August 23, 2022, MMH, MCRSC, and MASC will provide written notice of this potential data event to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, MMH, MCRSC, and MASC moved quickly to investigate and respond to the potential data privacy event, assess the security of relevant MMH systems, and identify potentially affected individuals. Further, MMH, MCRSC, and MASC notified federal law enforcement regarding the event. MMH, MCRSC, and MASC are providing access to credit monitoring services for 1 year to potentially affected individuals in Maryland, at no cost to these individuals.

Additionally, MMH, MCRSC, and MASC are providing potentially affected individuals with guidance on how to better protect against identity theft and fraud. MMH, MCRSC, and MASC are 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. MMH, MCRSC, and MASC are providing relevant regulatory notices in this matter.

Contact Information

Should you have any questions regarding this notification or other aspects of the potential data event, please contact us at (267) 930-4799.

Very truly yours,

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/cob
Enclosure

EXHIBIT A



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97225

To Enroll, Please Call:
1-833-423-1796
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

August 23, 2022

<<NOTICE OF PRIVACY EVENT / DATA BREACH>>

Dear <<First Name>> <<Last Name>>,

<<Data Owner Long Name>> (“<<Data Owner Short Name>>” or “we”) are writing to make you aware of an event that may impact some of your information. This notice provides you with information about the event, our response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On July 5, 2022, we became aware of unusual activity on certain systems. Upon becoming aware of the unusual activity we promptly took steps to better ensure the integrity of our network and begin an investigation with the assistance of a third-party company. To date the investigation confirmed that an unauthorized actor accessed systems containing <<Data Owner Short Name>> data between May 20, 2022, and July 7, 2022, and copied certain files. Although the investigation is ongoing, as part of the response to this event, we are conducting a detailed review to determine what information was present in the relevant systems at the time of the unauthorized access and to whom those records relate. We continue to notify individuals as we identify potentially affected information, and this process is ongoing.

What Information Was Involved? The ongoing investigation has determined that the following types information relating to former staff members, former employees, and individuals who provided information as part of their medical credentialing may have been impacted by the event: name, address, Social Security number, driver’s license or state identification number, and medical history information. The information involved varies by individual depending on what the individual provided to <<Data Owner Short Name>> for purposes the individual’s involvement with <<Data Owner Short Name>>.

What We Are Doing. Information security is one of our highest priorities, and we have security measures in place to protect information in our care. We responded promptly when we became aware of this event by taking steps to secure our systems and commence a comprehensive investigation. We are also reviewing and enhancing existing policies and procedures and implementing additional safeguards to further secure the information in our systems. Additionally, we reported this event to federal law enforcement. As an added precaution, we are offering you access to <<12/24>> months of credit monitoring and identity protection services at no cost to you through IDX. You will find information on how to enroll in these services in the enclosed “Steps You Can Take To Protect Your Personal Information.” We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached “Steps You Can Take To Protect Your Personal Information.”

For More Information. If you have additional questions or concerns, please call our dedicated assistance line at 1-833-423-1796, from 8 a.m. to 8 p.m. Central Time. Please know we take this event very seriously and sincerely regret any inconvenience or concern it may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Robin Winebar". The signature is fluid and cursive, with a large initial "R" and "W".

Robin Winebar
Interim President and CNO

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is November 23, 2022.

Telephone. Contact IDX at 1-833-423-1796 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

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:

Full name (including middle initial as well as Jr., Sr., II, III, etc.);

1. Social Security number;
2. Date of birth;
3. Addresses for the prior two to five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
6. 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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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 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 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. MMH is located at 8000 W. Eldorado Parkway, McKinney, TX 75070. MCRSC is located at 6045 Alma Rd. Suite 100, McKinney, Texas 75070. MASC, now closed, was formerly located at 125 Raintree Cir. Suite 200, Allen, Texas 75013



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

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

October 7, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent Methodist McKinney Hospital (“MMH”) located at 8000 W. Eldorado Parkway, McKinney, Texas 75070. MMH first notified your office of a data privacy event on August 23, 2022. MMH supplemented its preliminary notice throughout the course of its investigation with the most recent being sent on August 26, 2022. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MMH does waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On July 5, 2022, MMH became aware of unusual activity on certain systems. An investigation was promptly commenced to better ensure the integrity of the systems and begin an investigation with the assistance of a third-party company. To date the investigation confirmed that an unauthorized actor accessed certain systems containing MMH data between May 20, 2022, and July 7, 2022, and copied certain files. As part of the response to this event, a detailed review was conducted to determine what information was present in the relevant systems at the time of the unauthorized access and to whom those records relate. MMH also reviewed their records and took steps to identify address information for purposes of providing individual notice. MMH notified individuals as information became available.

On or about September 15, 2022, MMH completed its most recent review effort and determined that the involved systems contain information including: name and medical information of an additional six (6) Maryland residents.

Notice to Maryland Residents

On or about October 7, 2022, MMH provided written notice of the potential data privacy event to six (6) additional Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. The total number of Maryland residents MMH has notified in this matter is forty-one (41).

Other Steps Taken and To Be Taken

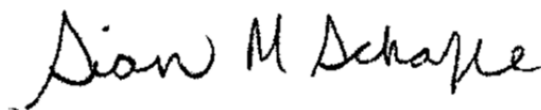
Upon discovering the event, MMH moved quickly to investigate and respond to the potential data privacy event, assess the security of certain MMH systems, and identify potentially affected individuals. Further, MMH notified federal law enforcement regarding the event. MMH is providing access to credit monitoring services for one (1) year to individuals whose personal information was potentially affected by this potential data privacy even, at no cost to these individuals.

Additionally, MMH is providing individuals with guidance on how to better protect against identity theft and fraud. MMH 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. Notice is also being provided to other relevant regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the potential data privacy event, please contact us at (267) 930-4799.

Very truly yours,

A handwritten signature in black ink that reads "Sian M Schafle". The signature is written in a cursive, flowing style.

Sian M. Schafle of
MULLEN COUGHLIN LLC

EXHIBIT A



P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-423-1796

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

October 7, 2022

<<NOTICE OF PRIVACY EVENT/DATA BREACH>>

Dear <<First Name>> <<Last Name>>,

Methodist McKinney Hospital (“MMH” or “we”) are writing to make you aware of an event that may impact some of your information. This notice provides you with information about the event, our response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On July 5, 2022, we became aware of unusual activity on certain systems. Upon becoming aware of the unusual activity, we promptly took steps to better ensure the integrity of our network and begin an investigation with the assistance of a third-party company. To date the investigation confirmed that an unauthorized actor accessed systems containing MMH data between May 20, 2022, and July 7, 2022, and copied certain files. Although the investigation is ongoing, as part of the response to this event, we are conducting a detailed review to determine what information was present in the relevant systems at the time of the unauthorized access and to whom those records relate.

What Information Was Involved? The ongoing investigation has determined that the following types of information relating to vendors of, and visitors to, MMH may have been impacted by the event: <<Data Element>>.

What We Are Doing. Information security is one of our highest priorities, and we have security measures in place to protect information in our care. We responded promptly when we became aware of this event by taking steps to secure our systems and commence a comprehensive investigation. We are also reviewing and enhancing existing policies and procedures and implementing additional safeguards to further secure the information in our systems. Additionally, we reported this event to federal law enforcement. As an added precaution, we are offering you access to <<12/24>> months of credit monitoring and identity protection services at no cost to you through IDX. You will find information on how to enroll in these services in the enclosed “Steps You Can Take To Protect Your Personal Information.” We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached “Steps You Can Take To Protect Your Personal Information.”

For More Information. If you have additional questions or concerns, please call our dedicated assistance line at 1-833-423-1796, from 8 a.m. to 8 p.m. Central Time. Please know we take this event very seriously and sincerely regret any inconvenience or concern it may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Robin Winebar". The signature is fluid and cursive, with a large initial "R" and "W".

Robin Winebar
Interim President and CNO

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is January 7, 2023.

Telephone. Contact IDX at 1-833-423-1796 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

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:

Full name (including middle initial as well as Jr., Sr., II, III, etc.);

1. Social Security number;
2. Date of birth;
3. Addresses for the prior two to five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
6. 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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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. MMH is located at 8000 W. Eldorado Parkway, McKinney, TX 75070.