

MARIETTA AREA HEALTH CARE INC. DBA MEMORIAL HEALTH SYSTEM PROVIDES NOTICE OF DATA PRIVACY EVENT

January 12, 2022

Marietta Area Health Care Inc. dba Memorial Health System (“MHS”) is providing notice of an incident that could affect the privacy of information of certain patients for whom it provided medical care. While MHS is unaware of any actual or attempted misuse of this information, MHS takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On August 14, 2021, MHS identified the presence of malware on certain servers in our environment. We immediately commenced an investigation to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that in connection with the malware event, an unauthorized actor accessed certain systems within our network on or about July 10 through August 15, 2021. On or about September 17, 2021, we determined the unauthorized actor may have accessed or acquired information from systems potentially containing patient information. We then carefully reviewed the contents of the affected systems to determine what, if any, sensitive information may have been compromised. On November 1, 2021, our review confirmed the scope of the information at risk and the population potentially impacted. We worked diligently since this time to confirm the patients who may be impacted, the types of information at issue, and the best contact information for the impacted population, in order to provide an accurate notification. On December 9, 2021, our review confirmed the impacted population and we began providing notice to affected individuals.

What Information Was Involved? We conducted a thorough review of the relevant systems to identify the types of information stored there and to whom it related. Our review determined that sensitive information was present in the affected systems and it is possible that this information could have been accessed or acquired by an unauthorized actor. While the specific data elements vary for each potentially affected individual, the scope of information potentially involved includes: name, date of birth, medical record numbers, patient account numbers, Social Security numbers, and other treatment and medical information. Although we have no reason to believe that any identity theft or unauthorized use of the affected information occurred, we wanted to provide notice of this incident.

How Will Individuals Know If They Are Affected By This Incident? We are mailing notice letters to the individuals identified as impacted. If an individual does not receive a letter but would like to know if they are affected, they may call our dedicated assistance line, detailed below.

What MHS is Doing. We have strict security measures to protect the information in our possession and have worked to add further technical safeguards to our environment. Following this incident, we took immediate steps to improve the security of our environment and increase our security posture.

Whom Should Individuals Contact For More Information? If individuals have questions or would like additional information, they may call our dedicated assistance line at (855) 545-2370 between the hours of 9:00 a.m. and 6:30 p.m., Eastern Standard Time, Monday through Friday.

What You Can Do? We encourage individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

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, military identification, 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 fraud alert or 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, D.C. 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. MHS is located at 401 Matthew Street, Marietta, OH 45750.

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 are 6 Rhode Island residents impacted by this incident.