EXHIBIT 1

By providing this notice, Marietta Area Health Care, Inc. dba Memorial Health System ("MHS") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 14, 2021, MHS identified the presence of malware on certain servers in its environment. MHS immediately commenced an investigation to determine the full nature and scope of the incident and to secure its network. Through this investigation, MHS determined that in connection with the malware event, an unauthorized actor accessed certain systems within its network on or about July 10 through August 15, 2021. On or about September 17, 2021, MHS determined the unauthorized actor may have accessed or acquired information from systems potentially containing patient information. MHS then carefully reviewed the contents of the affected systems to determine what, if any, sensitive information may have been compromised. On November 1, 2021, this review confirmed the scope of the information at risk and the population potentially impacted. MHS 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, this review confirmed the impacted population.

The information that could have been subject to unauthorized access includes name, address, Social Security number, medical/treatment information, and health insurance information.

Notice to Maine Residents

On or about January 12, 2022, MHS began providing written notice of this incident to all affected individuals, which includes twenty-six (26) Maine residents. 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, MHS moved quickly to investigate and respond to the incident, assess the security of MHS systems, and notify potentially affected individuals. MHS is also working to implement additional safeguards and training to its employees. MHS is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MHS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. MHS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

EXHIBIT A

MEMORIAL HEALTH SYSTEM

COMMUNITY • HEALTH • EXCELLENCE • LIFE

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Header)>>

Dear <<first_name>> <<last_name>>:

Marietta Area Health Care Inc. dba Memorial Health System ("MHS") writes to inform you of an incident that may affect the privacy of some of your information. We are providing you with an overview of the incident, our response, and steps you may take to better protect yourself, should you wish 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 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 have 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 determined that protected information related to you may have been impacted.

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 your information was present in the affected systems and it is possible that your information could have been accessed or acquired by an unauthorized actor. This information includes your <<b2b_text_2(data elements)>>. While we have no reason to believe that any identity theft or unauthorized use of the affected information has occurred, we wanted to make sure you are aware of this incident.

What We Are Doing. MHS has strict security measures to protect the information in our possession, and we 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.

As an added precaution, we are also offering you complimentary access to 12 months of identity monitoring services, through Kroll. You will need to activate these services yourself if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Personal Information* for additional information on these services.

What You Can Do. We encourage you to review the enclosed *Steps You Can Take To Help Protect Your Personal Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. We also encourage you to activate the complimentary identity monitoring services we are offering you. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.

For More Information. If you have questions about this letter, please call (855) 545-2370 between the hours of 9:00 a.m. and 6:30 p.m., Eastern Time, Monday through Friday, excluding major U.S. holidays.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Scott Cantley
President & CEO
www.mhsystem.org

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Activate Identity Monitoring Services

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(EnrollmentDeadline)>> to activate your identity monitoring services.

Membership Number: **<<MembershipNumber (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

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:

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, 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 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 [#] Rhode Island residents impacted by this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.