EXHIBIT 1

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, Singing River Health System 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 19, 2023, Singing River was the victim of a malicious and sophisticated ransomware attack. We promptly took steps to secure our systems, and with the assistance of third-party forensic specialists, conducted an investigation to confirm the nature and scope of the incident. Through the investigation, we identified unauthorized access within our environment between August 16 and August 18, 2023. Following this determination, we are notifying all individuals whose information may have been included in the impacted files. Although we have no indication of any misuse of your personal information as a result of this event, out of an abundance of caution, we are providing notice to individuals who may have been impacted. The information that could have been subject to unauthorized access includes name, date of birth, address, Social Security number, medical information, and health insurance information.

Notice to Maine Residents

On or about January 12, 2024, Singing River Health System began providing written notice of this incident to thirty-eight (38) residents. Supplemental notice was provided on October 18, 2023. 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, Singing River Health System moved quickly to investigate and respond to the incident, assess the security of Singing River Health System systems, and identify potentially affected individuals. Further, SRHS notified federal law enforcement regarding the event. Singing River Health System is also working to implement additional safeguards and training to its employees. Singing River Health System is providing access to credit monitoring services for twelve (12) months through IDX identity theft protection, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Singing River Health System 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. Singing River Health System 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.

Singing River Health System is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Singing River
Health System

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

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/singingriver

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

January 12, 2024

<<NOTICE OF [DATA EVENT] / [DATA BREACH]>>

Dear <<First Name>> <<Last Name>>:

Singing River Health System, for itself and on behalf of its wholly owned subsidiary Singing River Gulfport (collectively "Singing River"), is writing to inform you of a data security incident that may have impacted some of the information stored within our computer environment. We take this issue seriously and are providing you with information about the event and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On August 19, 2023, Singing River was the victim of a malicious and sophisticated ransomware attack. We promptly took steps to secure our systems, and with the assistance of third-party forensic specialists, conducted an investigation to confirm the nature and scope of the incident. Through the investigation, we identified unauthorized access within our environment between August 16 and August 18, 2023. Following this determination, we are notifying all individuals whose information may have been included in the impacted files. Although we have no indication of any misuse of your personal information as a result of this event, out of an abundance of caution, we are providing notice to individuals who may have been impacted.

What Information Was Involved? The investigation determined that the information potentially impacted *may* include your name, date of birth, address, Social Security number, medical information, and health information. We have no evidence that any of your information was used for identity theft or fraud.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the incident, we promptly took steps to confirm our system security, and engaged with a third-party forensic specialist to assist in conducting a comprehensive investigation. As an added precaution, we are offering <<12/24>> months of credit monitoring and identity restoration services through IDX. If you wish to activate these complimentary services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information*. If you elect to activate these services, you must enroll in these services directly as we are unable to act on your behalf to do so.

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 over the next 12 to 24 months.

For More Information. If you have additional questions or concerns, please feel free to call us at 1-888-996-3921, scan the QR code above, or go to https://response.idx.us/singingriver. We are available Monday through Friday from 8 am – 8 pm Central Time. You may also write to us at 3109 Bienville Blvd., Ocean Springs, Mississippi 39564, with attention to the Legal Department.

Sincerely,

Singing River Health System

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/singingriver and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is April 12, 2024.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership 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, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-996-3921 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported promptly to law enforcement and the relevant 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 https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 16 Rhode Island residents that may be impacted by this event.