EXHIBIT 1

By providing this notice, Tift Regional Health System, Inc. ("Tift") 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 or around August 16, 2022, Tift became aware of suspicious activity affecting certain systems within its network. Tift immediately launched an investigation, with the assistance of third-party computer forensic specialists, to confirm the full nature and scope of the activity. Tift disabled the network proactively as a security response and restored access quickly. There was no encryption of systems or access to Tift's electronic medical record system, and the network remained available for staff and patients to support care delivery and services. The investigation determined that certain files on Tift's systems were or may have been accessed or copied without authorization between August 11, 2022 and August 17, 2022. Tift thereafter undertook a time intensive and thorough review of the documents at risk, and recently completed this process.

The information that could have been subject to unauthorized access includes name, date of birth, Social Security number, and medical information.

Notice to Maine Residents

On or about August 11, 2023, Tift started providing written notice of this incident to fifteen (15) 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, Tift moved quickly to investigate and respond to the incident, assess the security of Tift systems, and identify potentially affected individuals. Further, Tift notified federal law enforcement regarding the event. Tift continues to implement additional safeguards and training to its employees. Tift is providing access to credit monitoring services for 12 months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Tift is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Tift 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.

Tift 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. Tift also notified the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

Christopher K. Dorman, FACHE
President/CEO
901 East 18th Street
Tifton, Georgia 31794
229-382-7120
MySouthwell.com

<<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 (NOTICE OF DATA BREACH/SECURITY INCIDENT)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Tift Regional Health System, Inc. ("Tift") is writing to notify you of an incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this event, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? On or around August 16, 2022, Tift became aware of suspicious activity affecting certain systems within our network. We immediately launched an investigation, with the assistance of third-party computer forensic specialists, to confirm the full nature and scope of the activity. We disabled the network proactively as a security response and restored access quickly. There was no encryption of systems or access to Tift's electronic medical record system, and the network remained available for staff and patients to support care delivery and services. The investigation determined that certain files on Tift's systems were or may have been accessed or copied without authorization between August 11, 2022 and August 17, 2022. We thereafter undertook a time intensive and thorough review of the documents at risk, and recently completed this process.

What Information Was Involved? Our investigation determined the following types of information related to you may have been impacted by this incident: your <<b2b_text_2 ("name" and data elements)>>. At this time, we have no indication that your information was used to commit identity theft or fraud as a result of this incident and are providing this notice out of an abundance of caution.

What We Are Doing. Data privacy and security are among Tift's highest priorities, and there are extensive measures in place to protect the information in our care. Upon discovery, we promptly commenced an investigation with the assistance of third-party computer forensic specialists to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying potentially impacted individuals. As part of our ongoing commitment to the privacy of information in our care, we continue to review our policies, procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities where necessary.

As an added precaution, we are also offering 12 months of complimentary access to credit monitoring services through Experian. Individuals who wish to receive these services must enroll by following the attached enrollment instructions as we are not able to enroll you 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 over the next 12 to 24 months. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you.

For More Information. If you have additional questions, please call our dedicated assistance line at (866) 676-3190**,** tollfree Monday through Friday 8:00 a.m. to 5:30 p.m. Central Time, (excluding major U.S. holidays). Be prepared to provide your engagement number **<<b2b_text_3 (engagement number)>>.**

Sincerely,

Christopher K. Dorman
President/CEO

https://mysouthwell.com

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

Ensure that you **enroll by** <<b2b_text_6 (activation date)>> (Your code will not work after this date.)

- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **<<Activation Code s_n>>**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by <<b2b_text_6 (activation date)>>. Be prepared to provide engagement number <<b2b_text_3 (engagement number)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 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/. Tift is located at 901 E. 18th Street, Tifton, GA 31794.

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 5 Rhode Island residents that may be impacted by this event.