EXHIBIT A

SAINT ANTHONY HOSPITAL

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<DATE>>

Re: Notice of Data <<Variable Data 4>>

Dear <<Full Name >>:

Saint Anthony Health Ministries ("Saint Anthony") is writing to provide you with notice of a data security event that may impact some of your information. We are providing you with information about the event, our response to it, and steps you can take to protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. Si su idioma principal es español, puede encontrar información sobre este incidente en nuestro sitio web SAHChicago.org o recibir información sobre el incidente llamando al centro dedicado de llamadas que se detalla a continuación.

What Happened? On December 18, 2023, Saint Anthony became aware of suspicious activity within its computer network. Immediate action was taken to secure our network, ensure that patient care was not disrupted, and investigate to determine the nature and scope of the activity with assistance from industry-leading cybersecurity specialists. On January 7, 2024, the investigation determined that files containing patient information had been copied from our network by an unknown actor on December 18, 2023. Thereafter, Saint Anthony provided notice of this incident to the public via our website homepage and appropriate news media outlets on January 30, 2024. We also conducted a thorough and time-intensive review of the involved files to identify names and address information for individuals with sensitive information involved. That review was recently completed.

What Information Was Involved? Our investigation determined that the following types of your information may have been impacted by this incident: <<Breached elements +Variable Data 1 + Variable Data 2>> and name. At this time, we are not aware of any identity theft or fraud in relation to this incident.

What We Are Doing. Saint Anthony holds cybersecurity and the privacy of patient information in our care as top priorities. Our prompt response to this event allowed us to continue providing patient care without disruption. As part of our ongoing commitment to data privacy, we are working to review existing policies and procedures and implement additional ones as needed. We promptly reported this incident to the FBI and are cooperating with their investigation. We also reported this incident to appropriate regulators, including the U.S. Department of Health and Human Services.

As an added precaution, we are offering you access to <<CM Duration>> of credit monitoring and identity protection services through CyEx. If you wish to activate the credit monitoring services or learn more about this offer, please see the enclosed *Steps You Can Take to Protect Your Personal Information.*

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Your Personal Information*, which contain information on what you can do to protect against the possibility of identity theft and fraud. You can also enroll to receive the complimentary credit monitoring and identity protection services being offered. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. If you have questions about this incident that are not addressed in this notice, please call our toll-free dedicated assistance line at 888-368-7518, 9:00am – 9:00pm EST, Monday through Friday, excluding holidays.

Sincerely,

Saint Anthony Health Ministries

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring

Identity Defense

<<Name 1>>
Enter your Activation Code: <<ActivationCode>>
Enrollment Deadline: <<Deadline>>
Service Term: <<CM Duration>>*

Identity Defense Complete – Key Features:

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions – To enroll in Identity Defense, visit: app.identitydefense.com/enrollment/activate/sahm

1. **Enter your unique Activation Code** <<ActivationCode>>

   Enter your Activation Code and click 'Redeem Code'.

2. **Create Your Account**

   Enter your email address, create your password, and click 'Create Account'.

3. **Register**

   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. **Complete Activation**

   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Deadline>>. After **<<Deadline>>**, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at **866.622.9303**.

* Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
** Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. 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 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 one-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 credit 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 fraud alert or 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	1-800-916-8800
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

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; 1-410-576-6300 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 <<Rhode Island Count>> Rhode Island residents that may be impacted by this event.