SAINT ANTHONY HOSPITAL

Saint Anthony Hospital is issuing notice of a recent data security event, which is still under investigation and may impact certain patients' information. As we continue to investigate and work toward notifying impacted patients directly, 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.

What happened? On December 18, 2023, Saint Anthony became aware of suspicious activity within our computer network. We took immediate action to secure the 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 the network by an unknown actor on December 18, 2023.

As a result, Saint Anthony undertook a thorough and time-intensive review of the involved files in order to identify and notify potentially impacted patients, which is still ongoing at this time. Though specific types of information impacted are unknown, there has been no indication that the hospital's Electronic Medical Record (EMR) database or financial systems as a whole were compromised. Once this review is complete, we will continue to work as quickly as possible to mail a notification letter directly to potentially impacted patients, which will include access to free credit monitoring and identity protection services.

Which patients / what information was affected? Saint Anthony's review is still ongoing to determine which patients and what types of information were potentially impacted by this incident. Once more is learned, we will provide updated information and mail notification letters to potentially impacted patients.

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

What affected individuals can do. While we are still working to determine the number of Saint Anthony patients involved, potentially impacted patients are encouraged to remain vigilant against incidents of identity theft. Review your account statements and explanations of benefits for unusual activity and to report any suspicious activity promptly to your insurance company, health care provider, or financial institution. Additional details can be found below in the *Steps You Can Take to Help Protect Your Information*.

For More Information. If you have additional questions, please call the dedicated assistance line we have established at 1-888-368-7518, Monday through Friday, between 8 a.m. and 8 p.m. Central Time. Or to speak to someone directly with Saint Anthony Hospital you can call 1-888-211-6763.

SAINT ANTHONY HOSPITAL

Steps You Can Take to Help Protect Your Information

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 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:

SAINT ANTHONY HOSPITAL

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	1-833-395-6938
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.