

Contact Us

Notice of Privacy Event

St. Anthony Regional Hospital - Notice of Data Privacy Event

St. Anthony Regional Hospital (“St. Anthony”) is providing notice of a recent event that may impact the confidentiality of information related to certain current or former patients. Although St. Anthony presently has no evidence that any such information has been used to commit identity theft or fraud, we are providing information about the event, the steps we have taken in response, and resources available to individuals to help protect information from possible misuse, should they feel it is appropriate to do so.

What Happened? On August 26, 2024, we became aware of suspicious activity affecting certain systems within our computer network. We immediately launched an investigation to confirm the full nature and scope of the activity with the assistance of industry-leading cybersecurity specialists. We also promptly notified federal law enforcement. The investigation determined there was unauthorized access to a subset of our network between August 14, 2024 and August 28, 2024, and that certain files within the network were accessed or downloaded without authorization during that time.

We are currently undertaking a comprehensive review to determine the information that may have been present in the potentially impacted files and to whom the information relates. Once complete, we will notify potentially affected individuals identified through the review process via written letter.

About Us

[Our Mission](#)

[Philosophy & Values](#)

[History & Heritage](#)

[Hospital Board of Directors](#)

[Leadership Team](#)

[St Anthony Ministries](#)

[Support Us](#)

[Community Health Needs Assessment](#)

[Receive St. Anthony News](#)

[Frequently Asked Questions](#)



What Information Was Involved. The investigation into the affected information is ongoing. The information that may have been present in the impacted files during the event varies by individual and could have included: full name, address, date of birth, Social Security number, financial information, medical information including treatment and diagnosis information.

What St. Anthony is Doing. St. Anthony takes this event and the security of information in our care very seriously. Upon learning of this event, we promptly commenced an investigation and took remediation actions. As part of our ongoing commitment to the privacy of information in their care, we are reviewing our policies, procedures, and processes to reduce the likelihood of a similar future event. We also reported the event to appropriate governmental agencies, including federal law enforcement and the U.S. Department of Health and Human Services.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should be promptly reported to the appropriate health care provider, insurance company, or financial institution. Additional information can be found below in the Steps You Can Take to Help Protect Personal Information.

For More Information. If you believe you are potentially affected by this event and have additional questions, you may contact St. Anthony toll-free at 833-794-5056; by email at privacy@stanthonyhospital.org; or by mail at P.O. Box 628, 311 South Clark St., Carroll, Iowa 51401.

Steps You Can Take To Help Protect Personal Information

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; 1-410-576-6300 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. Fees may be required to be paid to the consumer reporting agencies.



[General](#)

[Services](#)

[Find a Doctor](#)

[Patients &](#)

[Visitors](#)

[Classes & Events](#)

[News](#)

[Locations](#)

[Contact Us](#)

[Join Our Team](#)

[Why St. Anthony](#)

[Career](#)

[Opportunities](#)

[Benefits](#)

[Our Community](#)

[Volunteers](#)

[Student](#)

[Experiences](#)

[Education](#)

[Partnership](#)

[Resources](#)

[About Us](#)

[Our Mission](#)

[Our](#)

[Commitments](#)

[Philosophy &](#)

[Values](#)

[History &](#)

[Heritage](#)

[St. Anthony](#)

[Ministries](#)

[Hospital](#)

[Board of](#)

[Directors](#)

[Leadership](#)

[Team](#)

[Community](#)

[Health Needs](#)

[Assessments](#)

[\(CHNA\)](#)

[Frequently](#)

[Asked Questions](#)

[For Employees](#)

[HealthStream](#) 

[Email](#) 

Receive Updates

Submit your email to receive St. Anthony news.

Subscribe

Copyright © 2024 St. Anthony Regional Hospital. All Rights Reserved.



[IHA Hospital](#)

[Charges Compare](#)

[Notice of Privacy](#)

[Practices](#)

[Price Transparency](#)

Legally known as St. Anthony

Regional Hospital and Nursing Home

[Site by Spinutech](#) 

