

NOTICE OF DATA PRIVACY EVENT

January 27, 2023 (Updated August 3, 2023) - Hayward Sisters Hospital d/b/a St. Rose Hospital (“St. Rose Hospital”) is providing notice of an event that impacts the privacy of certain individuals’ information. St. Rose Hospital takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On or around November 29, 2022, St. Rose Hospital discovered suspicious activity on our computer systems. In response, we immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party computer forensic specialists. The investigation determined that an unknown actor gained access to certain computer systems on our network and acquired certain files from those systems on or about November 18, 2022. We identified the affected files on December 13, 2022, and undertook a comprehensive and time-consuming review of the files in order to identify the type of information contained therein, and to whom the information relates. On April 12, 2023, we completed this extensive review process and identified that information pertaining to certain current and former patients was present in the affected files. Since then, we have been performing additional work to review and verify the affected information as well as locate address information in order to provide direct notice to as many impacted individuals as possible.

What Information Was Involved? While we have no evidence of any actual or attempted fraudulent misuse of information as a result of this incident, our review determined that the following types of information were present in the affected files that were accessed and acquired by the unauthorized actor: name, Social Security number, driver’s license number, passport number, date of birth, medical/health information, treatment information, prescription information, health insurance information, and payment card information. The type of information at issue varies for each person.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. Federal law enforcement is aware of this incident, and we are cooperating with their investigation. We are notifying impacted individuals for whom we have a valid mailing address via U.S. mail and offering them credit monitoring and identity protection services. We are also notifying applicable regulators, including the U.S. Department of Health and Human Services.

How Will Individuals Know If They Are Affected By This Incident? St. Rose Hospital is mailing a notice letter to individuals whose information was determined to be in the affected files, for whom we have a valid mailing address. If an individual does not receive a letter but would like to know if they are affected, they may call our dedicated assistance line, detailed below.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

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 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

Website Notice

law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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 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 More Information. If individuals have questions or would like additional information, they may call St. Rose Hospital's dedicated assistance line at (833)-324-2449 between the hours of 6:00 a.m. to 8:00 p.m. Pacific time, Monday through Friday, or 8:00 a.m. to 5:00 p.m. Pacific time, Saturday and Sunday. This excludes all major U.S. holidays.