WVU Medicine
THOMAS HOSPITALS

THOMAS MEMORIAL HOSPITAL

4605 MacCorkle Avenue, SW
South Charleston, WV 25309

Notice of Data Incident

September 29, 2023

Upon information and belief, on or about July 7, 2021, Thomas Memorial Hospital ("TMH") received notice from CaptureRx, a third party partner in processing pharmacy claims, of a security incident involving a subset of files containing patient information. CaptureRx has since retrieved the information and received confirmation from the perpetrator that no copies were retained. To date, CaptureRx is unaware of any actual or attempted misuse of the affected information. In response to the incident, CaptureRx, on behalf of certain TMH contracted pharmacies, notified certain affected individuals of the incident.

Despite the steps taken by CaptureRx, TMH wanted to ensure each affected TMH patient received the appropriate notice. After thoroughly reviewing all steps taken by CaptureRx and the TMH contracted pharmacies, TMH notified certain individuals via mail who did not receive notification of the incident from CaptureRx or one of the TMH contracted pharmacies. These letters provided affected individuals information about the event, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so. This Notice of Data Incident is to serve as substitute notice for those individuals we attempted to notify but were ultimately unable to reach. It contains the same information regarding the incident as the notification letters.

What Happened? In February 2021, CaptureRx became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its systems. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021, without authorization.

CaptureRx then immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx completed this review to confirm the full scope of affected individuals and associated covered entities to which the information related.

In 2022, CaptureRx also notified affected individuals of this incident by alerting them to their potential eligibility in a class action settlement resulting from the incident. However, to further ensure that individuals were aware of this incident, on May 5, 2023, TMH began notifying on a rolling basis those affected individuals who did not receive notification of the incident from CaptureRx or one of the TMH contracted pharmacies.

What Information Was Involved? The investigation determined that, at the time of the incident, the relevant files contained first name, last name, date of birth, and prescription information. CaptureRx has assured TMH that no sensitive information, such as social security numbers or individual (member) insurance identification numbers, were affected.

What Is TMH Doing? Upon learning of this incident, TMH communicated extensively with CaptureRx regarding the incident. To ensure each affected TMH patient received the appropriate notice of the incident, TMH has thoroughly reviewed all steps taken by CaptureRx and the TMH contracted pharmacies, and has attempted to notify certain individuals who did not receive notification of the incident from CaptureRx or one of the TMH contracted pharmacies. TMH is committed to ensure that all potentially affected individuals receive the appropriate notice.

What You Can Do. Although we have no evidence or reason to believe that any of the affected information is being utilized in an unauthorized manner, we encourage individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors.

For More Information. TMH's Director of Corporate Compliance is available to answer any questions individuals may have at: 1-877-872-8254 (toll free), Monday – Friday, 9:00 a.m. to 5:00 p.m., Eastern Time.

STEPS YOU CAN TAKE TO PROTECT PERSONAL 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 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 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 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	1-833-395-6938
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 West Virginia's Attorney General's Office's Consumer Protection Hotline at 1-800-368-8808. This notice has not been delayed by law enforcement.