**Notice Hosted on the Tri-City Healthcare District Website**

Notice of Data Incident

Tri-City Healthcare District (“Tri-City”) experienced a data security incident that may affect the privacy of certain patient data.

On November 9, 2023, Tri-City detected suspicious activity on its network and immediately began an investigation. The investigation included the assistance of third-party specialists and determined an unknown party accessed certain files within Tri-city’s network on or about November 8, 2023. Tri-city then conducted a comprehensive review of the files at issue to determine whether personal information may have been involved. After a thorough review of the impacted data, on September 27, 2024, it was determined that some of your personal information was present in the impacted data set.

Tri-city’s review included the assistance of third-party data review specialists and determined the potentially impacted information included the following types of information related to patients: name, address, date of birth, Social Security number, medical treatment/diagnosis information, dates of service, health insurance provider name, health insurance claim information, and/or treatment cost.

Tri-City has provided written notice of this incident via First Class U.S. Mail to patients for whom Tri-City has been provided a valid address. In response to this incident, Tri-City notified law enforcement and implemented additional security measures to further minimize the risk of a similar incident occurring in the future. While Tri-City has no reason to believe any of the information described above has been misused, in an abundance of caution, Tri-City is providing individuals access to Single Bureau Credit Monitoring/Credit Report/Credit Score services at no charge. These services provide potentially impacted individuals with alerts when changes occur to their credit file. This notification is sent the same day that the change or update takes place with the bureau. Tri-City is also providing potentially impacted individuals with proactive fraud assistance to help with any questions potentially impacted individuals might have, or in event that someone becomes a victim of fraud. These services will be provided by IDX a company specializing in fraud assistance and remediation services.

Individuals who received a written notification letter or believe they might be impacted by this incident may also contact Tri-City’s dedicated assistance line at 1-888-783-9173, between the hours of 6:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday, excluding holidays, or write to Tri-City at 4002 Vista Way, Oceanside, CA 92056.

In general, Tri-City encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing credit reports/account statements and explanation of benefits forms 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, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228.

Individuals have the right to place an initial or extended fraud alert on a credit file at no cost. If individuals are a victim of identity theft, they are entitled to an extended fraud alert lasting seven years. As an alternative to a fraud alert, they have the right to place a credit freeze on a credit report. The credit freeze is designed to prevent credit, loans, and services from being approved without consent. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on your credit report.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

**TransUnion Experian Equifax**

1-800-680-7289 1-888-397-3742 1-888-298-0045

www.transunion.com www.experian.com www.equifax.com

You can further educate yourself regarding identity theft, fraud alerts, credit freezes and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.