Maria Efaplomatidis, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C 402
Brooklyn, NY 11201
mefaplomatidis@constangy.com

April 4, 2024

VIA ONLINE SUBMISSION
Attorney General Rob Bonta
Office of the Attorney General
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Re: Notification of Data Breach

Dear Attorney General Bonta:

Constangy, Brooks, Smith, and Prophete LLP represents Tri-City Healthcare District ("Tri-City") in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in compliance with California's data breach notification statute.

1. Nature of the Security Incident

On November 9, 2023, Tri-City became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, Tri-City took steps to secure its digital environment. Tri-City also engaged leading cybersecurity experts to assist with an investigation and to determine whether personal information may have been accessed or acquired without authorization. The investigation revealed that an unknown actor may have gained access to certain data from the Tri-City network on or about November 8, 2023. Tri-City then worked with additional experts to conduct a comprehensive review to determine what personal information was involved. On or about March 7, 2024, Tri-City learned that files containing personal information may have been accessed in connection with this incident.

2. Number of Affected California Residents Notified

On April 4, 2024, Tri-City notified 7143 California residents by letter mailed via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

The impacted information may include the residents' names and social security numbers.

3. Measures Taken to Address the Incident

In response to the incident, Tri-City retained cybersecurity experts and launched a forensics investigation to determine the source and scope thereof. Tri-City implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. Tri-City also notified the Federal Bureau of Investigation and U.S. Department of Homeland Security, and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible.

Tri-City is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity

protection services to each individual whose personal information was affected by this event, including 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. Those services are offered through IDX, A Zero Fox Company, the data breach and recovery services expert. IDX will also support a call center for at least 90 days to answer questions and assist with enrollment.

4. Contact Information

Tri-City takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 718.719.6475 or mefaplomatidis@constangy.com.

Sincerely yours,

Maria Efaplomatidis of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Consumer Notification Letter

PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>> <<Suffix>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/TriCity

April 4, 2024

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear << First Name>> << Last Name>> <<Suffix>>:

Tri-City Healthcare District ("Tri-City") is writing to inform you of a recent data security incident that may have involved your personal information. We take the privacy and security of all information within our possession very seriously. Although we have no evidence that your information has been misused for identity theft or fraud as a result of this incident, out of an abundance of caution, we are providing you with steps you can take to help protect your personal information and are offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On November 9, 2023, Tri-City became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, we took steps to secure our digital environment. We also engaged leading cybersecurity experts to assist with an investigation and to determine whether personal information may have been accessed or acquired without authorization. The investigation revealed that an unknown actor may have gained access to certain data from the Tri-City network on or about November 8, 2023. Tri-City then worked with additional experts to conduct a comprehensive review to determine what personal information was involved. On or about March 7, 2024, we learned that files containing personal information may have been involved in connection with this incident.

What Information Was Involved? The information involved included your name along with your Social Security Number.

What We Are Doing As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation, U.S. Department of Homeland Security and will provide whatever cooperation is necessary to hold the perpetrators accountable, if possible.

Tri-City is also notifying you of this incident and offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX, A Zero Fox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll scan the QR image, go to https://response.idx.us/TriCity and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter or call 1-888-783-9173. The deadline to enroll in these services is July 4, 2024. IDX representatives are available Monday through Friday from 6:00 am to 6:00 pm Pacific Time.

What You Can Do: We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: IDX Representatives are available until July 4, 2024, to assist you with questions regarding this incident, between the hours of 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, excluding holidays. Please call the help line at 1-888-783-9173 and supply the specialist with your unique code listed above.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Tri-City Healthcare District
4002 Vista Way
Oceanside, CA 92056

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://www.marylandattorneygeneral.gov/
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf