Notice of Data Event

Native American Health Center (Website Notice)

Native American Health Center ("NAHC") is providing this substitute notice as a result of a security incident to provide individuals with information about the incident and to share resources available for those who wish to further safeguard their personal information.

A security incident occurred at a third-party company ("TriZetto") that works with NAHC's electronic medical record system ("OCHIN"). On December 9, 2025, OCHIN issued a notice to NAHC concerning the TriZetto security incident. Importantly, NAHC did not receive the notice until December 15, 2025. On December 15, 2025, NAHC learned an unknown individual gained unauthorized access to one of TriZetto's systems which contained information concerning some of NAHC's patients. It is NAHC's understanding that TriZetto took immediate steps to secure its systems after discovering the breach.

Immediately after NAHC learned of the event, NAHC began working closely with OCHIN to understand what happened, prevent this issue from reoccurring, and identify any sensitive or personal information that may have been impacted as a result. Since that time, NAHC has been working diligently and exhaustively to identify and obtain sufficient information in order to provide you with this notice.

Based on the information received from TriZetto and OCHIN, the data involved may have included some sensitive personal information such as: Name, Social Security number, date of birth, contact information, and certain health or insurance information. Importantly, there is no evidence any information has been misused. Starting on January 5, 2026, notification letters were mailed to the patients NAHC identified as potentially being impacted. The individualized letters explain what personal information may have been impacted because of this incident.

Starting February 9, 2026, TriZetto will provide a dedicated, toll-free call center for questions. Individuals who have questions and who would like to learn if their data may have been affected may call 1 (844) 572-2724 Monday through Friday from 8 a.m. to 5:30 p.m. Central Time, excluding holidays.

Although NAHC is unaware of any actual or attempted misuse of any information, it is providing notice of this incident out of an abundance of caution and in compliance with applicable laws. Impacted individuals will also receive free credit monitoring, cyber monitoring, and identity theft protection services to those impacted by this incident.

Privacy and security are our top priorities. We deeply regret that this incident occurred and will continue to implement the most stringent security protocols available to prevent incidents like this one in the future. For additional information and guidance, please review the Reference Guide below to help protect your personal information.

Please reference the below FAQs for more information:

ABOUT THE TRIZETTO PROVIDER SOLUTIONS DATA BREACH

- **Who:** TriZetto Provider Solutions (TPS), a technology vendor for healthcare, suffered a breach exposing patient data.
- **What happened:** Hackers accessed TPS' web portals, stealing Protected Health Information (PHI) and Personally Identifiable Information (PII).
- **Impact:** Affects many healthcare organizations including Native American Health Center and their patients/members; potential risk for identity theft.
- **Kroll's Role:** Kroll was hired by TPS to provide identity theft monitoring and restoration services to affected individuals, hence the connection in notifications. Affected patients will receive a separate letter from Kroll and/or TPS that includes a unique code and instructions to enroll in credit monitoring services.

FREQUENTLY ASKED QUESTIONS

Q: Was Native American Health Center hacked?
A: No. Native American Health Center (NAHC) did not have a breach of its system. A business we use to help us with billing services called TriZetto Provider Solutions (TPS) noticed their system was impermissibly accessed.

Q: What happened with the breach?
A: TPS became aware of suspicious activity within a web portal that some of its business partners use to access its systems.

Q: When did the breach happen?
A: October 2, 2025. TPS immediately investigated and fixed the issue. During its investigation TPS discovered the activity began in November 2024. TPS notified NAHC on December 15, 2025.

Q: Was my information involved?
A: NAHC sent letters to patients whose information was involved. If you did not receive a letter and your address with us is up-to-date, your information was not involved.

Q: What specific items of my personal information were involved?
A: Varying combinations of names, addresses, birthdates, Social Security numbers, health insurance member numbers (which, for some individuals, may be a Medicare beneficiary identifier), provider names, health insurer names, primary insured information, and other demographic, health, and health insurance information. The incident DID NOT affect any payment card, bank account, or other financial information.

Q: What is NAHC doing about the breach? How will NAHC prevent this from happening in the future?
A: The breach happened to TPS. NAHC's system was not hacked or accessed. Our system has been reviewed and is secure.

Q: Does this mean that I'm a victim of identity theft?
A: No. The fact that someone may have had access to your information doesn't mean that you are a victim of identity theft or that your information will be used to commit fraud. We wanted to let you know about the incident so that you can take appropriate steps to protect yourself. The way to protect yourself is to place a fraud alert on your credit files, order your credit reports, and review them for possible problems.

Q: How will I know if any of my personal information was used by someone else?
A: The best way to find out is to order your credit reports from the three credit bureaus: Equifax, Experian and Trans Union. If you notice accounts on your credit report that you did not open or applications for credit ("inquiries") that you did not make, these could be indications that someone else is using your personal information, without your permission.

Q: Do I have to pay for the credit reports?
A: No. You can order your credit reports from all three credit bureaus for free once a year. You can do this online at www.annualcreditreport.com, or by phone at 1-877-322-8228.

Q: What can I do?
A: You can place a fraud alert on your credit files. Simply call any one of the three credit bureaus at the numbers provided below and follow the "fraud victim" instructions. The one you call will notify the others to place the alert.
• Equifax 1-888-766-0008
• Experian 1-888-397-3742
• TransUnion 1-800-680-7289

Q: What else can I do to protect myself?
A: Although we have no evidence that any of your information has been subject to identity theft or fraud, you should always remain alert by regularly reviewing your account statements and monitoring free credit reports and immediately reporting to your banks and other financial institutions any suspicious activity involving your accounts. For more resources visit: https://www.irs.gov/identity-theft-fraud-scams/identity-protection.
We also encourage you to enroll in the identity monitoring services that Kroll will offer to you soon.

Q: What is TPS doing?
A: TPS assured us that after becoming aware of the incident, it immediately took additional protective measures to safeguard its systems and worked with leading cybersecurity experts to conduct a comprehensive investigation of the incident. TPS notified law enforcement and is cooperating with their investigation. TPS has eliminated the threat to the environment. To help prevent similar incidents from happening in the future, TPS implemented and is continuing to implement additional security protocols designed to enhance the security of its services.

Q: The notice is addressed to my child, who is a minor. What should I do?
A: See the California Department of Justice's information sheet When Your Child's Identity Is Stolen on the Identity Theft page at https://oag.ca.gov/idtheft/facts/childs-identity

Q: The notice is addressed to my spouse, who is deceased. What should I do?
A: See the California Department of Justice's information sheet Identity Theft and the Deceased on the Identity Theft page at https://oag.ca.gov/idtheft/facts/deceased

FOR MORE INFORMATION OR QUESTIONS REGARDING THE BREACH, PLEASE CONTACT:

TriZetto's dedicated toll-free call center: (844) 572-2724.

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 303485281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will

reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, GA 30348	1-888-766-	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA	1-800-680- 7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.
Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up to date. Please be sure and tell your provider's office

when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Additional Information

Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Contact the District of Columbia Office of Attorney General for steps to avoid identity theft: (202) 727-3400, 400 6th Street, NW, Washington DC 20001, http://oag.dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Maryland Attorney General: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

Massachusetts Residents: You have the right to obtain a police report and request a free security freeze as described above.

New York Residents: You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 or 1-800-7889898; https://ag.ny.gov/. You also may contact the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.

North Carolina Residents: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov.

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401- 274-4400.

South Carolina Residents: You can obtain information from the South Carolina Department of Consumer Affairs: 293 Greystone Blvd., Ste. 400, Columbia, SC 29210; 800-922-1594; www.consumer.sc.gov.

Texas Residents: You can obtain information from the Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621- 0508; www.texasattorneygeneral.gov/consumer-protection/.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

New Mexico: You have rights pursuant to the Fair Credit Reporting Act. These rights include knowing what is in your file and your credit score; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; to be told if information in your credit file has been used against you; as well as other rights. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. For more information about the FCRA, and your rights pursuant to the FCA, please visit https://files.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.