

Native American Health Center Notice of Data Security Incident

[<https://www.nativehealth.org/>]

Native American Health Center (“NAHC”) has become aware of a data security Incident that may have resulted in an unauthorized access to your sensitive personal information. While we have not received any report of fraudulent misuse of the information, NAHC sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

What Happened? On November 19, 2023, NAHC was the victim of a cybersecurity incident. Upon discovery of this incident, NAHC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. In January 2024, the forensic investigation found evidence to suggest that some NAHC files were accessed by an unauthorized actor.

Based on the findings of the forensic investigation, NAHC began an extensive and comprehensive review of the potentially affected files and folders to identify what information was impacted. This review identified that some individuals’ information may have been impacted by this incident. On May 28, 2024, NAHC finalized the list of individuals to notify and identified their addresses to the extent available. Notice was mailed out to identified individuals on June 3, 2024.

What Information Was Involved? The information impacted varied by individuals but included name, address, medical information, or Social Security number. A formal notice letter has been sent to those who have had their sensitive information impacted, and the identified the types of information involved.

What We Are Doing. Data privacy and security is among NAHC’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, NAHC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, NAHC took the following steps, including but not limited to: implement a comprehensive measure to replace all hard drives in every workstation to enhance overall security; continue the use of multifactor authentications for all logins, a measure already in place prior to the breach; continue annual HIPAA privacy & security risk assessments; extend the deployment of a multifactor authentication system that will replace the use of passwords with the scan of a fingerprint or tap of a badge (currently in pilot in select departments); uphold restricted access to all IT department offices & server rooms for heightened physical activity; maintain the practice of restricted access & ongoing monitoring for buildings and sites equipped with key card access, ensuring controlled and monitored entry; and conduct ongoing annual reviews of policies, procedures, employee training programs that cover cybersecurity, HIPAA compliance & privacy, took steps and will continue to take steps to mitigate the risk of future harm.

If there was unauthorized access to sensitive information, NAHC will be offering complimentary credit monitoring and identity theft protection services to those impacted individuals. Notification letters were sent to those impacted individuals with the information to enroll in the credit monitoring services. NAHC strongly encourages all identified individuals to register for this free service.

What You Can Do. NAHC encourages all members to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that individuals contact his/her financial institution and all major credit bureaus to inform them of such a breach and take the recommended steps to protect his/her interests, including the possible placement of a fraud alert on the credit file.

For More Information. NAHC recognizes that our members may have questions not addressed in this notice. For more information, please call 1-833-543-2507 (toll free) Monday through Friday, during the hours of 5:00 a.m. and 5:00 p.m. Pacific Time (excluding U.S. national holidays).

Sincerely,
Native American Health Center

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian		TransUnion		Equifax		
P.O.	Box	9554P.O.	Box	2000P.O.	Box	105069
Allen,	TX	75013Chester,	PA	19016Atlanta,	GA	30348
1-888-397-3742		1-800-680-7289		1-800-525-6285		
www.experian.com/fraud/center.html		www.transunion.com/fraud-alerts		https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/		

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian		TransUnion		Equifax		
P.O.	Box	9554P.O.	Box	2000P.O.	Box	105069
Allen,	TX	75013Chester,	PA	19016Atlanta,	GA	30348
1-888-397-3742		1-800-680-7289		1-800-525-6285		
www.experian.com/fraud/center.html		www.transunion.com/fraud-alerts		https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/		

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Vermont: 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).

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-9995630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

New York Office of Attorney General - you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina Office of the Attorney General - the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1401-274-4400; www.riag.gov