FOR IMMEDIATE RELEASE
January 3, 2020

Media Contact
Sue Van Brocklin or Lance Heisler / Coates Kokes
sue@coateskokes.com, lance@coateskokes.com, 503.241.1124

Malicious malware targets Native American Rehabilitation Association of the Northwest

NARA NW informs patients of potential data security breach

PORTLAND, Ore.—Today the Native American Rehabilitation Association of the Northwest, Inc. (NARA NW) announced that it experienced a cybersecurity incident November 4-5, 2019, that appears to have resulted in unauthorized access of some patient healthcare information. This incident – which involved a phishing email attack that contained a computer malware called Emotet – affected the email accounts of some NARA NW staff members. The U.S. Department of Homeland Security describes Emotet as among the most costly and destructive malware affecting state, local and tribal governments, as well as the private sector. It is a malicious program capable of accessing and exporting email messages, as well as attachments connected with email messages. Some of the NARA NW email accounts affected by the virus contained records with patient information.

Based on its investigation to date, with support from a digital forensics and cybersecurity firm, NARA NW has identified 344 or approximately 1.3 percent of current or former patients in NARA NW's electronic records whose information appears to have been accessed without authorization or were at an increased risk of unauthorized access. Some of these patients' information was contained in the text of email messages, while other patients' information was contained only in attachments to emails. Although there is not a clear indication that these email attachments were accessed, NARA NW, out of an abundance of caution, is treating the information in these attachments as though it were accessed and notifying the patients accordingly. The types of information that were contained in these records include names, home addresses, birth dates, Social Security numbers, and medical record or patient ID numbers. Additionally, some records include patient clinical information, such as diagnoses, services or treatment, and treatment dates.

In addition, there is a second group of clients and patients to whom NARA NW is providing notice: patients whose types of information as described above was potentially affected, but there is no indication this information was actually accessed. To be extra cautious and in the interest of protecting its patients and providing transparency, NARA NW is notifying all of the patients in this second category as well.

NARA NW is mailing written notices to these two groups of clients and patients. If you have questions about the incident, including whether your information was affected, **you can call NARA NW toll-free at 1-866-361-5795 from 9 a.m. to 5 p.m., Monday-Friday.**

"As we've all heard in the news, hackers and malicious computer programs are increasingly targeting all kinds of organizations—from giant retail stores to banks, and certainly many healthcare organizations," said Jacqueline Mercer, CEO of NARA NW. "It is sad that there are people in the world whose intent is to cause harm and distress to vulnerable populations such as our clients. Words cannot express how truly sorry we are that our clients and NARA NW have been subjected to this malware attack. We take our responsibility to protect and take care of our clients and their personal information very seriously. We have launched a thorough investigation and are working with cybersecurity experts and law enforcement to get to the bottom of this."

What happened

On November 4, 2019, some NARA NW staff members received emails containing malware that bypassed NARA NW's security system and affected their email accounts. NARA NW learned about the incident on the afternoon of November 4 and began working to contain it. Based on the available evidence, the threat posed by the malware was contained by November 5. After learning about this incident, IT staff at NARA NW investigated, contained and removed the malware from the organization's network, restricted network access, and required users to reset their passwords by November 6. After the malware was removed from the affected computers by their antivirus software, NARA NW also applied an additional endpoint protection solution to all NARA NW computers to monitor them for any suspicious activity that could be related to malicious software. As part of its response, NARA NW also promptly engaged cybersecurity consultants and forensic investigators to analyze and understand the incident and to protect the private information of employees and clients. NARA NW has notified law enforcement of the incident and is continuing to work with them.

During November and December, cybersecurity consultants and digital forensic investigators continued to review emails and attachments that were potentially accessed to analyze the incident and to help NARA NW understand what happened and how to better protect patient information.

Mercer emphasized that for the vast majority of patients, there is no indication that records containing their information were actually accessed. In addition, she said it is important to note that a lot of information in their organization's records may relate to individuals' involvement with NARA NW as staff members, volunteers, supporters or active community members, rather than client healthcare records. NARA NW is conducting a thorough review of its information

privacy and security policies and procedures to reduce the risk of future incidents and plans to provide additional and ongoing training to all of their employees in an effort to prevent any future incidents.

NARA NW has provided written notice to all potentially affected individuals, notified local media, and informed government authorities with which it works. It also has established a dedicated call center within the organization, managed by staff members knowledgeable about this incident and the services that NARA NW provides to patients. If any current or former patients have any questions or concerns about this incident, **they are encouraged to call NARA NW toll-free at 1-866-361-5795 from 9 a.m. to 5 p.m., Monday-Friday.**

What you can do to protect your information

You should always be vigilant when receiving and responding to correspondence or inquiries from unknown sources. You should regularly monitor your financial accounts and healthcare information for any unusual activity. If you notice any unusual activity, you should immediately notify your financial institutions (for example, your bank or credit card provider) and your healthcare providers.

In addition, please carefully review the "Identity Theft Prevention and Protection" summary below of additional steps you can take to protect your personal information, which includes recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It also includes the contact information for the three major credit reporting agencies and suggestions for obtaining and reviewing your credit report.

About NARA NW

Founded in 1970 in Portland, Oregon, the Native American Rehabilitation Association of the Northwest, Inc. is an Indian-owned, Indian-operated, non-profit agency. Originally an outpatient substance abuse treatment center, NARA NW now operates a residential family treatment center, an outpatient treatment center, a child and family services center, a primary healthcare clinic, several adult mental health locations, a wellness center, and transitional housing for Native women and children. All services are centered on the family as it is NARA NW's philosophy that, without the family circle there will be no future.

Traditional Indian culture and spirituality have always been an integral part of NARA NW's services. In recognition of their service to American Indian and Alaska Natives, NARA NW has been honored with a sacred pipe, a totem pole, sacred fire circle and a drum. The pipe and drum continue to be used in sacred ceremonies; the totem pole stands at the entrance of their residential facility. It is NARA NW's philosophy to honor and support the emotional, physical, spiritual and mental health of Indian people.

The mission of NARA NW is to provide education, physical and mental health services and substance abuse treatment that is culturally appropriate to American Indians, Alaska Natives and anyone in need.

###

IDENTITY THEFT PREVENTION AND PROTECTION

Monitor Your Accounts and Credit Reports, and Notify Police and the FTC of Suspicious Activity:

When you receive account statements, credit reports, and monitoring alerts, review them carefully for unauthorized activity. Look for accounts you did not open, unauthorized purchases, inquiries from creditors that you did not initiate, and personal information that you do not recognize, such as a home address or Social Security number. If you have concerns, call your bank, the account provider, or the credit reporting agency. If possible, place a security verification secret word, similar to a password, on your accounts.

If you suspect any fraudulent activity or identity theft, promptly report it to local law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to https://www.consumer.ftc.gov/features/feature-0014-identity-theft or call 1-877-ID-THEFT (877-438-4338). Request copies of any police or investigation reports created, as you might need to provide this information to credit reporting agencies or to supposed creditors to clear up your records.

***Obtain Free Credit Reports*:** Even if you do not find any signs of fraud on your reports, you should check your credit report regularly. There are three main credit reporting agencies: Equifax, Experian, and TransUnion. Their contact information, along with contact information for the FTC and some state agencies, are on the reverse side. Each credit reporting agency must provide you annually with a free credit report, at your request made to a single, centralized source for the reports, AnnualCreditReport.com. You are not required to order all three reports at the same time; instead, you may rotate your requests so that you can review your credit report on a regular basis. In addition, many states have laws that require the credit reporting agencies to provide you with a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

***Free Services by Credit Reporting Agencies*:** Each credit reporting agency offers additional free services to help you protect your credit. TransUnion at www.transunion.com permits you to sign up for TrueIdentity which is a service that allows you to examine your TransUnion credit file and place a "credit lock" which prevents others from opening up credit in your name. Experian at www.experian.com provides you with a free credit report every month when you select "Start with your free Experian Credit Report." Equifax at www.equifax.com permits you to sign up for "Lock & Alert" which also allows you to place a credit lock.

***Fraud Alert*:** You may ask the credit reporting agencies to place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three credit reporting agencies. As soon as that agency processes your fraud alert, it is supposed to notify the other two, which then also must place fraud alerts in your file. An *initial fraud alert* stays in your file for at least 90 days. An *extended alert* stays in your file for seven years. To place either of these alerts, a credit

reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency.

Security Freeze: You also have the right to place a security freeze on your credit report at any of the three main credit reporting agencies. 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 may be able to use an online process, an automated telephone line, or a written request. If you choose to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail, the following information must be included when requesting a security freeze: (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. 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, and displays your name, current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the agency. The main three credit reporting agencies provide details about their security freeze services and state requirements at the following links:

- Experian: http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/
- Equifax: https://help.equifax.com/app/answers/detail/a_id/159 & https://help.equifax.com/app/answers/detail/a_id/75/~/security-freeze-fees-and-requirements
- TransUnion: https://www.transunion.com/credit-freeze/place-credit-freeze

***Internal Revenue Service*:** Tax-related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund. If you received IRS correspondence indicating you may be a victim of tax-related identity theft or your e-file tax return was rejected as a duplicate, do the following:

- Submit an IRS Form 14039, Identity Theft Affidavit, to the IRS;
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039; and
- Watch for any follow-up correspondence from the IRS and respond quickly.

The fillable IRS Form 14039 is available at IRS.gov. Follow the instructions exactly. You can fax or mail it or submit it with your paper tax return if you have been prevented from filing because someone else has already filed a return using your SSN. You only need to file it once. Do not respond to threats made over the phone or via email that the IRS will take action against you. The IRS will communicate with you in writing.

***Financial Accounts, Oral Passwords and 2FA*:** If financial accounts are affected, contact the institution and ask them about steps you may take to further protect your account. Financial

institutions will often permit you to place an oral password on your account or enable multifactor authentication to your online account.

***Contact Information for the FTC, Credit Reporting Agencies, and State Consumer Protection Agencies*:**
If you suspect fraudulent activity on any of your financial accounts (savings, checking, credit card) or identity theft, you are encouraged to report your concerns to your financial institutions and the relevant agencies below.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

AnnualCreditReport.com
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
www.annualcreditreport.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com