



## **Data Breach Notification** **July 8, 2019**

In compliance with federal and State laws, this provides substitute notice.

Nemadji provides patient eligibility detection and billing services for the County of Los Angeles Department of Health Services (DHS). As a business associate of DHS, we respect the privacy of your information and take patient privacy very seriously. This notice is to inform you of a data breach that may involve the personal information of 14,591 DHS patients, and it is important to us that you are made fully aware of this recent event.

### **What Happened**

On March 28, 2019, a Nemadji employee fell victim to an email phishing attack. A phishing email tries to trick someone into giving up important information by appearing to come from a reliable source. Email accounts are used by Nemadji employees to communicate about and perform services for DHS. The phishing email compromised one email account and led to the current data breach. On June 26, 2019, Nemadji confirmed to DHS that the phishing attack may have impacted DHS patients but there is no evidence suggesting personal information relating to DHS patients was specifically targeted by the phishing event.

### **What Information Was Involved**

The personal information for DHS patients present in the email account at the time of the incident varied by individual but may have included first and last names and one or more of the following data elements: address, date of birth, phone number, patient account number, medical record number, admission and discharge dates, Medi-Cal identification number, month and year of service. The Social Security Number of two patients and diagnostic codes of four patients was also identified. No specific medical information was exposed.

### **What Nemadji Is Doing**

Nemadji values patient privacy and deeply regrets that this incident occurred. Upon discovering the breach, we immediately took steps to prevent further access and began working closely with cybersecurity vendors to ensure that the incident is properly addressed. Nemadji has initiated an administrative review, reviewed and revised processes to enhance security, and implemented additional controls designed to prevent the recurrence of such an incident. Additionally, Nemadji has also enhanced our workforce training to identify and respond to phishing emails.

In addition to notifying individuals potentially impacted by this incident, we notified the Federal Bureau of Investigation. We will also notify the State Attorney General's Office and the U.S. Department of Health & Human Services' Office for Civil Rights as required by law.

### **What You Can Do**

Although Nemadji is unaware of any actual or attempted misuse of information as a result of this incident, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring for potentially impacted individuals at no cost for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

To receive credit services by mail instead of online, impacted individuals may call 1-800-491-4740. Additional information describing services is listed below.

Please review the "Additional Resources" section below. This section describes additional steps you can take to help protect yourself, including 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.

### **For More Information**

If you have questions, please call 1-800-491-4740, Monday through Friday from 8:00 a.m. to 5:30 p.m. PT.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

## **ADDITIONAL RESOURCES**

### **Monitor Accounts**

We encourage individuals to remain vigilant against incidents of identity theft and fraud, to review your bank account statements, credit or debit card statements, health insurance policy statements, credit reports, and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

PO Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

**Experian**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19106  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

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](http://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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.