NOTICE OF DATA INCIDENT

NLACRC is providing notice of an incident that affected protected health information stored in our systems.

What Happened?

On November 28, 2024, we discovered suspicious activity on our systems with indicators consistent with a ransomware event. We immediately began an investigation and took steps to contain the situation. This included notifying federal law enforcement and engaging cybersecurity and privacy professionals to assist.

Currently, the investigation found evidence of unauthorized activity within NLACRC computer systems on November 20, 2024 through December 1, 2024, and took a copy of some information before encrypting or encoding certain computer systems to render them inaccessible. Our investigation determined that some personal information was copied from our systems. While there is currently no evidence of identity theft or fraud in relation to this incident, your trust is important to us.

What Information Was Involved?

Based on the current findings of the investigation, the following types of information for clients may have been impacted: first and last names, addresses, dates of birth, telephone numbers, social security numbers, email addresses, financial account information, payment card information, health plan numbers, health plan beneficiary numbers, health insurance information, full-face photos and/or comparable images, UCI and patient ID numbers (unique identifying number or code generated by us for you), medical information, lab results, medications, diagnosis and/or treatment information, treatment cost information, disability codes, and certificate/license numbers.

These are general categories of information that we believe may be present within the affected systems and may have been accessed by the unauthorized actor during the incident. However, specific individuals and the extent of the information accessed are not yet known. While our investigation is ongoing, we are providing this notice to all individuals who may potentially be affected by this situation.

What We Are Doing.

Upon becoming aware of the Incident, we immediately took steps to further improve the security of our systems and practices. This included enhancing our monitoring processes for increased protection from cybersecurity threats, changing passwords, and strengthening password practices. After determining that an unauthorized actor gained access to our systems, we immediately began analyzing available information to confirm the identities of potentially affected individuals and notify them. We added further technical safeguards to our existing protections, and brought systems back online as quickly and securely as possible. We continue to work with leading privacy and security firms to aid in our response, and we have reported this incident to relevant government agencies.

What Can Impacted Individuals Do?

The investigation is ongoing and the identities of individuals who were affected is not yet known. However, out of an abundance of caution, NLACRC encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Additional information and resources are outlined below.

If you have questions for NLACRC, you can contact the toll-free assistance line for our dedicated call center at 855-295-5618, Monday through Friday, from 6:00 a.m. to 6:00 p.m. PT (excluding some U.S. national holidays).

Steps You Can Take to Protect Your Personal Information

To obtain a free credit report, individuals may visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

Alternatively, affected individuals can contact the three (3) major credit reporting bureaus directly at the addresses below:

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

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

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

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your

credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

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 to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. Contact information for the Consumer Response Center of the Federal Trade Commission is 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/ or 1-877-IDTHEFT (438-4338).

Protecting Medical Information.

If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.