Keck Medicine of USC
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-814-1789
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 15, 2022

Re: Notice of Data <<Variable 1>>

Dear <<FirstName>> <<LastName>>,

We are writing to provide you with information about a recent data security incident that may have involved your personal or protected health information. At Keck Medicine of USC ("Keck"), we take the privacy and security of patient information very seriously. We are writing to notify you that this incident occurred, offer complimentary identity protection services, and inform you about steps you can take to help safeguard your information.

What Happened. On September 30, 2022, Keck learned of unusual activity involving a provider's email account. Upon discovering this activity, we immediately took steps to secure the account and launched an investigation with the assistance of an independent forensic investigator. The investigation revealed that the provider's email account was accessed without authorization on September 30, 2022. As a result, we undertook a review of the contents of the email account to determine what, if any, personal or protected health information may have been involved. On November 22, 2022, we learned that some of your information was contained within the account. Since that time, we have been diligently collecting up-to-date address information needed to notify all potentially affected individuals.

Please note that this unauthorized access was limited to information in a provider's work email account and did not affect any other Keck information systems. We are not aware of the misuse of any information that may have been involved in this incident.

What Information Was Involved. The potentially affected information may have included your <<variable text>>. Your Social Security number, driver's license number, and financial account information were not identified in the provider's email account.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. Keck has also assigned the provider additional security awareness training and is working to implement additional technical controls to reduce the likelihood of a similar incident reoccurring.

Additionally, Keck is providing you with information about steps that you can take to help protect your information and, as an added precaution, is offering you complimentary identity protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The deadline to enroll is March 15, 2023.

What You Can Do. We recommend that you activate your complimentary IDX services using the enrollment code provided above. A description of the services being provided is included with this letter. We also recommend that you review the guidance included with this letter about steps you can take to protect your information.

For More Information. If you have questions or need assistance, please contact IDX at 1-833-814-1789, Monday through Friday from 6:00 am to 6:00 pm Pacific Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your information.

Keck takes this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Ajay R. Vyas, Esq.
Chief Healthcare Compliance & Privacy Officer
Keck Medicine of USC

1510 San Pablo Street, Suite 600
Los Angeles, California, 90033
privacy@med.usc.edu

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

IDX Identity Protection Services

1. **Website and Enrollment**. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. **Activate the identity monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. *You must have access to a computer and the internet to use this service.* If you need assistance, IDX will be able to assist you.

3. **Telephone**. Contact IDX at 1-833-814-1789 to speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

IDX Identity will include one-year enrollment into the following service components:

1. CYBERSCAN - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like Social Security numbers, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
2. IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible.
3. FULLY-MANAGED IDENTITY RECOVERY - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.