Health Services
LOS ANGELES COUNTY

313 N. Figueroa Street, Suite 106
Los Angeles, CA 90012

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

We are writing to inform you of a cyberattack against the County of Los Angeles Department of Health Services ("DHS") that may affect the privacy of some of your personally identifiable and/or health information. DHS is taking this incident seriously and we are working and cooperating with law enforcement on this matter.

What Happened?

On February 6, 2024, DHS was the victim of a cyber-attack. Specifically, a hacker by-passed the multi-factor authentication safeguards of an employee's Microsoft 365 account through a method commonly referred to as "push notification spamming." We believe that the cyber-attack may have provided the attacker with access to certain personal information. Due to the ongoing investigation by law enforcement, we were directed to delay notifying the impacted parties of this incident, as public notice may have hindered their investigation. To address this matter proactively, we are providing detailed information on steps you can take to safeguard your personal information. Additionally, we have implemented enhanced security measures to prevent future occurrences. Your privacy and security are of utmost importance to us, and we are committed to maintaining the highest standards of protection for your information.

What Information Was Involved?

The information identified in the potentially compromised e-mail account may have included your first and last name, date of birth, home address, phone number, Social Security number, government issued identification, medical record number, medical information (e.g., diagnosis/condition, medication, treatment), and/or health insurance information. Each individual may have been impacted differently and not all the elements listed above were present for each individual.

What We Are Doing

DHS has implemented numerous enhancements and controls to minimize the risk of its exposure to similar cyber-attacks. Upon discovery of the phishing attack, we acted swiftly to disable the impacted user's e-mail account, reset and re-imaged the user's device(s), blocked websites that were identified as part of the phishing campaign and quarantined all suspicious incoming e-mails. Law enforcement was notified upon discovery of the phishing attack, and they initiated a criminal investigation. Additionally, awareness notifications were distributed to all DHS workforce members to be vigilant when reviewing e-mails, especially those including links or attachments.

Upon determination that the account had been compromised, DHS immediately initiated a comprehensive review and engaged an industry-leading forensic specialist to determine the extent of the breach and the type of information affected. Further, we enhanced training to identify and respond to phishing attacks as part of the DHS ongoing cyber-security awareness program.

In addition to notifying individuals potentially impacted by this incident, we will notify the U.S. Department of Health & Human Services' Office for Civil Rights, California Department of Public Health, the State Attorney General's Office, and other agencies as required by law and/or contract.

Data security and privacy are among our highest priorities, and we diligently work to stay ahead of the rapidly evolving and continuous threats to large data systems. DHS remains vigilant in its efforts to protect confidential information and continues to strengthen its information privacy and security program to implement safeguards to prevent and/or reduce cyber-attacks.

What You Can Do

While DHS cannot confirm that your information has been misused, we encourage you to remain vigilant and review the content and accuracy of the information in your medical record with your medical provider and be watchful for any suspicious activity on any of your accounts. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll, a global leader in risk mitigation and response, to provide identity monitoring for one year at no cost to you. Kroll and its team have extensive experience helping people who have sustained an unintentional exposure of confidential data.

Identity monitoring services available to you include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of the identity monitoring services available to you.

You have until <<b2b_text_6 (activation deadline)>> to activate the identity monitoring services.

Membership Number: <<Membership Number s_n>>

Additional information describing the services is included with this letter. For more information about Kroll and Identity Monitoring services, you can visit its website at: https://www.info.krollmonitoring.com/

The enclosed "Steps You Can Take to Help Protect Against Identity Theft and Fraud," provides additional information you can use to help protect your information.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. We have established a dedicated call center available toll free in the U.S. at 1-866-898-8099, from 6:00 a.m. to 5:00 p.m. Pacific Time (excluding weekends and major U.S. holidays). You may also visit the following website for more information: https://dhs.lacounty.gov

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Christina R. Ghaly, M.D.
Director, Los Angeles County Department of Health Services

STEPS YOU CAN TAKE TO HELP PROTECT AGAINST IDENTITY THEFT AND FRAUD

Review and Monitor Your Medical Information, Explanation of Benefits

We encourage you to review your medical record with your medical provider to make sure that the content is correct and accurate. You may also review the Explanation of Benefits' statement(s) that you receive from your health care provider or health plan. If you see any service(s) that you do not believe you received, contact your health care provider or health plan at the telephone number listed on the Explanation of Benefits' statement, or contact your health care provider or health plan and ask them to send you a copy of your statement after each visit.

Request Credit Reports

The County encourages you to remain vigilant against incidents of identity theft and fraud, to review your financial statements, and to monitor your credit reports 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 or call, toll-free, 1-877-322-8228. You may also contact the below three major credit bureaus directly to request a free copy of your credit report:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	800-916-8800
www.Equifax.com	www.Experian.com	www.transunion.com

The credit bureaus will ask for a Social Security Number (SSN) and other personal information for identification purposes. Once you contact a credit bureau, you will receive a letter with instructions on how to receive your free credit reports. Review the reports to make sure your personal information, such as, address and SSN are accurate. If there is anything you do not understand, call the credit reporting agency at the telephone number on the report and ask for an explanation.

If you find that your information has been misused, or that an account has been falsely created using your identity, contact the local police department, your bank, and your credit card agencies. You should obtain a copy of the police report in case you need to give copies of the police report to creditors to clear up records. Even if you do not find any signs of fraud on the reports, you should check your credit report every three months for the next year and call the credit bureau numbers above to order reports and keep the fraud alert (described below) in place.

Request Fraud Alerts

You, or your legal representative, can also have these credit bureaus place a Fraud Alert on your file that alerts creditors to take additional steps to verify your identity before granting credit in your name. Note, however, that because a Fraud Alert tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your Fraud Alert, the others are notified to place Fraud Alerts on your file. Should you wish to place a Fraud Alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed above.

Request a Security Freeze

You may also place a Security Freeze on your credit reports. A Security Freeze prohibits a credit bureau from releasing any information from your credit report without your written authorization. However, please be advised that placing a Security Freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. You will need to place a Security Freeze separately with each of the three major credit bureaus listed below if you wish to place a freeze on all of your credit files. A credit bureau is not allowed to charge you to place, lift, or remove a Security Freeze if you have been a victim of identity theft, and you provide the credit bureau with a valid police report. In all other cases, each credit bureau may charge you a fee to place, temporarily lift, or permanently remove a Security Freeze. To find out more on how to place a Security Freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com/personal/credit-report-services/credit-freeze/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
800-916-8800
www.transunion.com/credit-freeze

Additional Information

You can learn more about identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. 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); and TTY: 1-866-653-4261.

You can also contact the FTC at the information above if you need more information on how to file such a complaint. Instances of known or suspected identity theft should also be reported to local law enforcement and your State Attorney General. Visit the California Office of Privacy Protection for additional information on protection against identity theft: https://oag.ca.gov/privacy

KROLL

Take Advantage of Your Identity Monitoring Services

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U S residential address associated with your credit file.