COUNTY OF LOS ANGELES
Public Health

Substitute Notice of Data Breach

This is an announcement regarding a phishing attack against the County of Los Angeles, Department of Public Health ("DPH") that may affect the privacy of some personally identifiable and/or health information of certain DPH clients, employees, and other individuals. DPH takes this incident seriously and has cooperated with law enforcement on this matter.

What Happened?

Between February 19, 2024, and February 20, 2024, DPH experienced a phishing attack. Specifically, an external threat actor was able to gain log-in credentials of 53 DPH employees through a phishing e-mail. A phishing e-mail is a fraudulent e-mail that appears to come from a legitimate source with the goal of tricking the recipient into divulging sensitive data. In this case, the DPH employees clicked on the link located in the body of the e-mail, thinking that they were accessing a legitimate message from a trustworthy sender.

Due to an investigation by law enforcement, we were advised to delay notification of this incident, as public notice may have hindered their investigation.

What Information Was Involved?

The information identified in the potentially compromised e-mail accounts may have included DPH clients/employees/other individuals' first and last name, date of birth, diagnosis, prescription, medical record number/patient ID, Medicare/Med-Cal number, health insurance information, Social Security Number, and other financial information.

Affected individuals may have been impacted differently and not all of the elements listed were present for each individual.

What We Are Doing

DPH has implemented numerous enhancements to reduce our exposure to similar e-mail attacks in the future. Upon discovery of the phishing attack, we acted swiftly to disable the impacted e-mail accounts, 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. Additionally, awareness notifications were distributed to all DPH workforce members to remind them to be vigilant when reviewing e-mails, especially those including links or attachments. Law enforcement was notified upon discovery of the phishing attack, and they investigated the incident.

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 and other agencies as required by law and/or contract.

We are seeking to stay ahead of the rapidly evolving and continuous threats to large data systems. DPH 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 DPH cannot confirm that whether information has been accessed or misused, we encourage clients/employees/other individuals to review the content and accuracy of the information in their medical record with their medical provider.

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 affected clients.

Additionally, affected clients should review "Steps You Can Take to Protect Against Identity Theft and Fraud," to help protect their information.

For More Information

DPH clients and employees that would like to inquire if their information was impacted can contact the following established dedicated call center available toll free in the U.S. at 1-866-898-4312, from 6:00 a.m. to 5:00 p.m. Pacific Time (excluding weekends and major U.S. holidays).

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