SUBSTITUTE NOTICE OF DATA BREACH

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

The County of Los Angeles, Department of Health Service ("DHS") was subject to a malicious cyberattack that may affect the privacy of some of your personally identifiable and/or health information. On June 20, 2024, notices were mailed to the known physical addresses of the potentially impacted individuals. This notice provides information about the cyberattack and our response for individuals for whom we did not have sufficient information to notify by mail. 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 circumvented 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 full name, date of birth, home address, phone number(s), e-mail address, Social Security Number, government issued ID, medical record number, health insurance information (health plan and member number), and/or medical information (e.g., diagnosis/condition, medication, treatment, dates of service).

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

What We Are Doing

DHS 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 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, We initiated comprehensive review, with the assistance of an industry-leading forensic firm, to identify any personal information or personal health

information which may have been affected, and implemented additional controls to minimize the risk of future phishing attacks against DHS e-mail accounts.

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 have notified 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.

We are seeking 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 patients to review the content and accuracy of the information in their medical record with their medical provider, and that you remain vigilant 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 to provide identity monitoring at no cost to you 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.

For additional information, please review "Steps You Can Take to Protect Against Identity Theft and Fraud," posted on this website: https://dhs.lacounty.gov. If you feel your personal information is being improperly used, you can also contact local law enforcement to file a police report.

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