DEPARTMENT OF MENTAL HEALTH

hope. recovery. wellbeing.

JONATHAN E. SHERIN, M.D., Ph.D.
Director

Gregory C. Polk, M.P.A.
Chief Deputy Director

Curley L. Bonds, M.D.
Chief Medical Officer

Lisa H. Wong, Psy.D.
Senior Deputy Director

Connie D. Draxler, M.P.A.
Senior Deputy Director

April 21, 2022

Substitute Notice of Data Breach

The Los Angeles County Department of Mental Health was subject to a malicious cyberattack and certain client information was compromised. On April 21, 2022, we completed mailing individual notices to the current known physical addresses of impacted individuals. This notice provides information about the cyberattack and our response for individuals for whom we did not have sufficient contact information to notify by mail.

What Happened

Between October 19, 2021 and October 21, 2021, we were the victim of a cyber-attack. Specifically, a malicious actor or actors was able to obtain the log-in credentials for the Microsoft Office 365 accounts of three of our employees through a phishing email attack. The phishing emails originated from a trusted business partner whose email server the actor or actors had compromised and then used to send multiple phishing emails to our employees. We believe that the cyber-attack may have provided the attacker with access to certain personal information, as described below.

What Information Was Involved

The personal information that may have been affected includes name, address, date of birth, drivers' license number, social security number, medical and/or health information, health insurance information and/or financial account number. This information relates to certain DMH clients who may have been impacted differently.

What We Are Doing

Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we acted swiftly to disable the impacted accounts and reset the Microsoft Office 365 and multi-factor authentication credentials. We also notified law enforcement and cooperated with law enforcement's investigation. Once our investigation determined which accounts had been compromised, we initiated a comprehensive review, with the assistance of industry leading forensic specialists, to identify any personally identifying information or personal health information in the impacted email accounts.

On March 4, 2022, after delaying our investigation and notification at the request of law enforcement, we completed our investigation and determined that certain elements of personal

information may have been impacted by this event. We then undertook a comprehensive internal reconciliation of the records found to identify individuals and confirm contact information.

Following this incident, we are reviewing and updating our security policies, procedures, and controls. We have also notified Microsoft of the vulnerability in the Microsoft Office 365 multi-factor authentication that was exploited by the malicious actor or actors.

What You Can Do

Although we have no evidence that any personal information has been misused, we encourage potentially affected individuals to remain vigilant for any suspicious activity on any of their accounts. To protect against the possibility of identity theft or other financial loss, we encourage potentially affected individuals to review account statements, and to monitor credit reports for suspicious activity.

For more information about what you can do to protect yourself from identity theft, please refer to guidance from the U.S. Federal Trade Commission (FTC) on their website: https://www.identitytheft.gov/#/Info-Lost-or-Stolen

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 three major credit bureaus directly to request a free copy of your credit report.

You can place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze	P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348 1-888-378-4329 www.equifax.com/personnal/credit-report-services/credit-freeze

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit

file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 4500 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud	P.O. Box 2000 Chester, PA 19016 1-800-916-8800 www.transunion.com/fraud-alerts	P.O. Box 105069 Atlanta, GA 30348 1-888-378-4329 www.equifax.com/personnal/credit-report-services/credit-fraud-alerts

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's 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. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Visit the California Office of Privacy Protection for additional information on protection against identity theft: https://oag.ca.gov/privacy

For More Information

We sincerely regret any inconvenience or concern this incident has caused. If you 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 (855) 482-1577, Monday through Friday from 8 a.m. to 5 p.m. Pacific Time.