LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

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

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

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to provide you with information about a cybersecurity incident that the Los Angeles County Department of Mental Health (DMH) experienced on October 19, 2021. DMH is taking this incident seriously and we are working and cooperating with law enforcement on this matter. At this time, we have discovered no evidence of actual misuse of your information. This notice explains what happened, what information of yours may have been affected, what measures we are taking, and steps you can take in response.

What Happened

Phishing emails were sent from an unknown threat actor and affected three DMH employee email accounts. Phishing emails appear to look like a secure email communication and trick recipients into giving up important information. In this case, the DMH employees clicked on the link located in the body of the email, thinking that they were accessing legitimate secure emails from the senders.

Based on our investigation, we believe that the cyber-attack impacted certain personal information, as described below. Though we have no evidence to suggest that any personal information has been accessed or misused, out of an abundance of caution, we are notifying you of this cyber-attack and providing you information you can use to proactively take steps to protect yourself and your information.

At the request of law enforcement, we delayed our notification of this incident until their investigation was complete, as public notice may have hindered their investigation.

What Information Was Involved

Certain personal information may have been impacted by this cyber-attack, including your name, address, date of birth, driver's license, Social Security number, medical and/or health information, health insurance information, SSID student identifier, and/or financial account number. Individuals may have been impacted differently.

What We Are Doing

Upon learning of this cyber-attack, we immediately began an internal investigation into the attack and also notified law enforcement authorities. Further, we have taken proactive measures to contain and mitigate the issue, including deploying additional security measures and resetting all network credentials. Lastly, we will be reporting this incident to the U.S. Department of Health & Human Services Office of Civil Rights.

What You Can Do

Although we have no evidence that any of your personal information has been accessed or misused, we encourage you to remain vigilant for any suspicious activity on any of your accounts.

Monitor Your Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your financial account 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 three major credit bureaus directly to request a free copy of your credit report.

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

<<Date>> (Formato: mes, día, año)

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

Re: aviso de filtración de datos

Estimado/a <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Le escribimos para brindarle información sobre un incidente de seguridad cibernética que tuvo el Departamento de Salud Mental (DMH) del condado de Los Ángeles, el 19 de octubre de 2021. El DMH está tomando este incidente con seriedad y estamos trabajando y cooperando con las autoridades en este asunto. Hasta ahora, no hemos descubierto ninguna evidencia de uso indebido de su información. Este aviso explica lo que sucedió, qué información suya puede haberse visto afectada, qué medidas estamos tomando y las medidas que se pueden adoptar en repuesta.

¿Qué sucedió?

Un agente malicioso desconocido envió correos electrónicos de phishing que afectaron a tres cuentas de correo electrónico de empleados del DMH. Los correos electrónicos de phishing parecen una comunicación de correo electrónico segura y engañan a los destinatarios para que proporcionen información importante. En este caso, los empleados del DMH hicieron clic en el enlace ubicado en el cuerpo del correo electrónico, pensando que estaban accediendo a correos electrónicos legítimos y seguros de los remitentes. De acuerdo con nuestra investigación, creemos que el ataque cibernético afectó cierta información personal, como se describe a continuación. Aunque no tenemos evidencia que sugiera que se haya accedido o usado indebidamente ninguna información personal, por precaución le notificamos sobre este ataque cibernético y le proporcionamos información que puede usar para tomar medidas proactivas para protegerse y a su información. A solicitud de la policía, retrasamos nuestra notificación de este incidente hasta que completaran su investigación, ya que el aviso público podría haber obstaculizado su investigación.

¿Qué información se vio comprometida?

Cierta información personal puede haber sido afectada por este ataque cibernético, incluido su nombre, dirección, fecha de nacimiento, licencia de conducir, número de seguro social, información médica y/o de salud, información del seguro médico, identificador de estudiante SSID y/o número de cuenta financiera. Las personas pueden haber sido afectadas de distintas formas.

¿Qué estamos haciendo?

Al enterarnos de este ataque cibernético, comenzamos de inmediato una investigación interna sobre el ataque y también notificamos a las autoridades policiales. Además, hemos tomado medidas proactivas para contener y mitigar el problema, incluida la implementación de medidas de seguridad adicionales y el restablecimiento de todas las credenciales de la red. Por último, informaremos de este incidente a la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de EE. UU.

¿Qué puede hacer usted?

Si bien no tenemos evidencia de que se haya accedido o utilizado indebidamente su información personal, le recomendamos que permanezca atento a cualquier actividad sospechosa en cualquiera de sus cuentas.

Security Freeze: Steps You Can Take to Protect Your Personal Information

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 or want to learn more about placing a security freeze on your credit, please contact the major consumer reporting agencies listed below:

CREDIT MONITORING BUREAUS		
EXPERIAN	**TRANSUNION**	**EQUIFAX**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19016	Atlanta, GA 30348
www.experian.com/freeze	www.transunion.com/creditfreeze	www.equifax.com/personal/contact-us

We regret any inconvenience or concern this incident has caused. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-855-482-1577, Monday through Friday from 8:00 a.m. to 5:00 p.m. Pacific Time (excluding major U.S. holidays).

Sincerely,

Maurnie V. Edwards
HIPAA Privacy Officer
Los Angeles County Department of Mental Health

Monitoree sus cuentas

Para protegerse contra la posibilidad de robo de identidad u otra pérdida financiera, le recomendamos que se mantenga alerta, revise sus estados de cuenta financieros y controle sus informes de crédito para detectar actividades sospechosas. Conforme a la legislación estadounidense, usted tiene derecho a un informe crediticio anual gratuito de cada una de las tres principales agencias de informes crediticios. Para solicitar su informe crediticio gratuito, visite www.annualcreditreport.com o llame sin costo al 1-877-322-8228. También puede comunicarse directamente con las tres agencias principales de informes crediticios para solicitar una copia gratuita de su informe crediticio.

Seguridad Bloqueo: medidas adicionales que puede adoptar para proteger su información personal

Usted puede colocar un "bloqueo de seguridad" en su informe crediticio, que prohibirá que una agencia de informes de los consumidores divulgue la información en su informe crediticio sin su autorización expresa. El bloqueo de seguridad está diseñado para evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Sin embargo, debe tener en cuenta que el uso de un bloqueo de seguridad para controlar quién tiene acceso a la información personal y financiera de su informe crediticio puede retrasar, interferir o prohibir la aprobación oportuna de cualquier solicitud posterior que realice con respecto a un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que implique la concesión de un crédito. De conformidad con la ley federal, no se le puede cobrar por colocar un bloqueo de seguridad en su informe crediticio, ni tampoco por retirarlo. Si desea colocar un bloqueo de seguridad o si desea obtener más información sobre cómo colocar un bloqueo de seguridad en su crédito, comuníquese con las principales agencias de informes del consumidor que se enumeran a continuación:

OFICINAS DE MONITOREO DE CRÉDITO		
EXPERIAN	**TRANSUNION**	**EQUIFAX**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19016	Atlanta, GA 30348
www.experian.com/freeze	www.transunion.com/creditfreeze	www.equifax.com/personal/contact-us

Lamentamos cualquier inconveniente o preocupación que este incidente le haya ocasionado. Entendemos que puede tener preguntas sobre este incidente que no se abordan en esta carta. Si tiene más preguntas, llame al 1-855-482-1577 de lunes a viernes, de 8:00 a. m. a 5:00 p. m. hora del Pacífico (a excepción de los principales días festivos de EE. UU.).

Atentamente,

Maurnie V. Edwards
Oficial de privacidad de HIPAA
Departamento de Salud Mental del condado de Los Ángeles

Steps You Can Take to Protect Your Information

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account 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 three major credit bureaus directly to request a free copy of your credit report.

Security Freeze.

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**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

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 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information.

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. Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC. 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.

For all U.S. residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580, consumer.gov/idtheft, 877-IDTHEFT (877-438-4338), TTY: 866-653-4261. ***For California residents:*** Visit the California Office of Privacy Protection (oag.ca.gov/privacy) for more information to protect yourself against identity theft. ***For Maryland residents,*** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***For New Mexico residents,*** you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. ***For North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716- 6400, and online at www.ncdoj.gov. ***For Oregon residents:*** Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 877-877-9392. ***For Washington D.C. residents:*** Reach the Office of Attorney General for the District of Columbia at: 400 6th St. NW, Washington, DC 20001; 202-442-9828; https://oag.dc.gov.

This document includes an important notice. If you cannot read this attached document, please call (855) 366-0136 for translation help.

TAGALOG

Ang liham na ito ay naglalaman ng mahalagang impormasyon. Kung hindi ninyo nababasa ang kalakip na liham, mangyaring tumawag sa 1-855-366-0136 upang magkaroon ng tulong sa pagsasalin sa Tagalog/Filipino.

RUSSIAN

В этомписьмесодержитсяважнаяинформация. ЕслиВынеможетепрочитатьприлагаемоеписьмо, позвонитепономеру 1-855-366-0136, и Вамбудутпредоставленыуслугипереводанарусскийязык.

KOREAN

이서신에는중요한정보가포함되어있습니다. 동봉된서신을읽으실수없으면
1-855-366-0136 로전화하여한국어번역지원을받으십시오.

ARMENIAN

Այս նամակը պարունակում է կարևոր տեղեկություններ: Եթե ներփակ նամակըչեք կարող կարդալ, խնդրվում է կապվեք 1-855-366-0136 հեռախոսահամարով, օգնություն ստանալՀայերեն լեզվով:

CHINESE

这封信包含了重要信息。如果您无法阅读随附的信件，请致电1-855-366-0136 寻求广东话翻译援助。

這封信包含了重要信息。如果您無法閱讀隨附的信件，請致電1-855-366-0136 尋求廣東話翻譯援助。

VIETNAMESE

Thư này bao hàm thông tin quan trọng. Nếu quý vị không đọc được thư đính kèm, vui lòng gọi 1-855-366-0136 để được giúp đỡ thông dịch trong tiếng Việt.

CHINESE

这封信包含了重要信息。如果您无法阅读随附的信件，请致电1-855-366-0136 寻求普通话翻译援助。

這封信包含了重要信息。如果您無法閱讀隨附的信件，請致電1-855-366-0136 尋求國語翻譯援助。

IRANIAN/PERSIAN

اینnامهحاوی اطلاعاتمهمی میباشد. اگرنامهضمیمهرانمیتوانیدبخوانید, لطفاًبرای کمکبهزبانفارسی باشمارهتلفن – 1-855-366-0136
تماسبگیرید.

ARABIC

هذه الرسالة تحتوي على معلومات هامة. إذا لم تتمكن من قراءة الرسالة المرفقة، يرجى الاتصال على 1-855-366-0136 للحصول على مساعدة في الترجمة إلى العربية.