CHANGE
HEALTHCARE
P.O. Box 989728
West Sacramento, CA 95798-9728

August 5, 2024

F1R3-2110794 A
State Tn Funder
312 Rosa L Parks Ave R
Nashville, TN 37243-1102

Notice of Data Breach

To State Tn Funder:

We are sorry to tell you about a privacy event. This letter is from Change Healthcare ("CHC"). We work with many doctors, health insurance plans, and other health companies to help provide health services or benefits. This event may have involved your data.

What happened?
On February 21, 2024, CHC found activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began investigating right away, and hired a special team to help us. We also called law enforcement. We also turned off CHC's systems to help protect our customers and their individuals.

On March 7, 2024, we learned a cybercriminal was able to see and take copies of some data in our computer system. This happened between February 17, 2024 and February 20, 2024. We received files that were safe to look at on March 13, 2024.

What information was involved?
We have told our clients about this event. Starting on June 20, 2024, we also told our clients about what data may have been seen and taken. We encourage you to remain vigilant by checking bills and accounts. The data that may have been seen and taken includes contact information (such as name, address, date of birth, phone number, and email) plus one or more of the following:

- Health insurance data (such as health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers)
- Health data (such as medical record numbers, doctors, diagnoses, medicines, test results, images, care, and treatment)
- Billing, insurance claims and payment data (such as claim numbers, account numbers, billing codes, payment cards, financial and banking, and balance)
- Other personal data (such as Social Security number, driver's license or state ID number, or other ID number)

The data that may have been seen and taken was not the same for everyone. Some of this data may be about the person who paid the bill for health care services.

Why did this happen?
A cybercriminal accessed our computer system without our permission.

What is CHC doing?
We investigated and called law enforcement. We are also making our computer systems even stronger than before. We do not want this to happen again.

We would like to offer you free credit monitoring and identity theft protection services. We will pay for the cost of this service for 2 years so that it is free for you. We have attached steps on how to sign up for this free service.

What you can do:
You can sign up for the free credit monitoring and identity protection services. Be sure that bills and accounts look correct. We have attached steps on how to do that. If you learn of a crime against you, you can file a report with law enforcement.

What if I have a question?
If you have any questions or concerns, please call us toll free at 1-866-262-5342. You can also learn more at changecybersupport.com. We are sorry for any concern this event may cause.

Sincerely,

Change Healthcare Privacy Office

CHANGE
HEALTHCARE
P.O. Box 989728
West Sacramento, CA 95798-9728

August 5, 2024

F1R3-2110794 A
State Tn Funder
312 Rosa L Parks Ave R
Nashville, TN 37243-1102

Aviso de filtración de datos

Para State Tn Funder:

Lamentamos informarle sobre una filtración de datos . Esta carta es de Change Healthcare ("CHC"). Trabajamos con muchos médicos, planes de seguro médico y otras compañías de salud para brindar servicios o beneficios de salud. Este evento puede haber involucrado sus datos.

¿Qué sucedió?
El 21 de febrero de 2024, CHC detectó que hubo actividad en nuestro sistema informático sin nuestro permiso. Rápidamente tomamos medidas para detener dicha actividad. Comenzamos a investigar de inmediato y contratamos a un equipo especial para que nos ayudara. También llamamos a la policía. Asimismo, desactivamos los sistemas de CHC para proteger a nuestros clientes y a sus personas.

El 7 de marzo de 2024, nos enteramos de que un ciberdelincuente pudo ver y tomar copias de algunos datos en nuestro sistema informático. Esto sucedió entre el 17 de febrero de 2024 y el 20 de febrero de 2024. Recibimos archivos que eran seguros para consultar el 13 de marzo de 2024.

¿Qué información se vio involucrada?
Les informamos a nuestros clientes sobre este evento. A partir del 20 de junio de 2024, también informamos a nuestros clientes sobre qué datos pudieron haberse visto y extraído. Le recomendamos que permanezca alerta revisando las facturas y cuentas. Los datos que se pudieron haber visto y extraído incluyen información de contacto (como nombre, dirección, fecha de nacimiento, número de teléfono y correo electrónico) y uno o más de los siguientes detalles:

- Datos del seguro médico (como planes/pólizas de salud, compañías de seguros, números de identificación de miembros/grupos y números de identificación de pagadores del gobierno de Medicaid-Medicare)
- Datos de salud (como números de historias clínicas, médicos, diagnósticos, medicamentos, resultados de pruebas, imágenes, atención y tratamiento)
- Facturación, reclamaciones de seguros y datos de pago (como números de reclamación, números de cuenta, códigos de facturación, tarjetas de pago, datos financieros y bancarios, y saldo)
- Otros datos personales (como el número de Seguro Social, la licencia de conducir o el número de identificación estatal, u otro número de identificación)

Los datos que se pudieron haber visto y extraído no eran los mismos para todos. Algunos de estos datos pueden ser sobre la persona que pagó la factura de los servicios de atención médica.

¿Por qué ocurrió esto?
Un ciberdelincuente accedió a nuestro sistema informático sin nuestro permiso.

¿Qué está haciendo CHC?
Investigamos y llamamos a la policía. También estamos reforzando nuestros sistemas informáticos aún más que antes. No queremos que esto vuelva a suceder.

Nos gustaría ofrecerle servicios gratuitos de monitoreo de crédito y protección contra el robo de identidad. Pagaremos el costo de este servicio durante 2 años para que sea gratis para usted. Hemos adjuntado los pasos a seguir para registrarse en este servicio gratuito.

Qué puede hacer usted:
Puede suscribirse a los servicios gratuitos de monitoreo de crédito y protección de identidad. Verifique que las facturas y las cuentas sean correctas. Se adjuntan los pasos sobre cómo hacerlo. Si se entera de un delito en su contra, puede presentar una denuncia ante la policía.

¿Y si tengo una pregunta?
Si tiene alguna pregunta o inquietud, llámenos al número gratuito 1-866-262-5342. También puede obtener más información en changecybersupport.com. Lamentamos cualquier preocupación que este evento pueda causar.

Atentamente.

Change Healthcare Privacy Office

ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-866-262-5342 (TTY: 1-866-262-5342).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-866-262-5342 (TTY: 1-866-262-5342).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-866-262-5342 (TTY: 1-866-262-5342)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 11-866-262-5342 (TTY: 1-866-262-5342).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-866-262-5342 (TTY: 1-866-262-5342).

注意:如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-866-262-5342 (TTY: 1-866-262-5342)。

ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-866-262-5342 (ATS : 1-866-262-5342).

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-866-262-5342 (TTY: 1-866-262-5342).

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-866-262-5342 (телетайп: 1-866-262-5342).

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 1- 866-262-5342 (رقم هاتف الصم والبكم: 1-866-262-5342).

ATTENZIONE: In cask la lingua palatal said litigant, so no disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-866-262-5342 (TTY: 1-866-262-5342).

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 1-866-262-5342 (TTY: 1-866-262-5342).

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-866-262-5342 (TTY: 1-866-262-5342)번으로 전화해 주십시오.

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-866-262-5342 (TTY: 1-866-262-5342).

સુચના: જો તમે ગુજરાતી બોલતા હો, તો નિ:શુલ્ક ભાષા સહાય સેવાઓ તમારા માટે ઉપલબ્ધ છે. ફોન કરો 1-866-262-5342 (TTY: 1-866-262-5342).

เรียน :ถา้ คุณพดู ภาษาไทยคุณสามารถใชบ้ ริการช่วยเหลือทางภาษาไดฟ้ รี โทร 1-866-262-5342 (TTY: 1-866-262-5342).

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in IDX Credit and Identity Monitoring Services

As a safeguard, you may enroll, at no cost to you, in online credit monitoring and identity restoration services provided by IDX for two years. To enroll in these services, please call CHC at 1-866-262-5342 and ask to enroll.

Individuals must enroll in order for the available services to go into effect, and the monitoring included in the membership must be activated to be effective. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days