HIPAA WEBSITE SUBSTITUTE NOTICE

Change Healthcare

NOTICE OF DATA BREACH (June 20, 2024; updated July 29, 2024 and August 8, 2024)

This notice is from Change Healthcare (CHC) about a recent security incident. Change Healthcare provides services to health care providers, health insurance plans and other companies, from which individuals may have received health services or health insurance. Because Change Healthcare works as a vendor to health care providers or health insurance plans, personal information, including health information, has been impacted in this incident.

CHC is posting this substitute notice to provide customers and individuals with information about the criminal cyberattack on CHC systems and to share resources available to people who believe their personal data potentially being impacted.

The review of personal information potentially involved in this incident is in its late stages. CHC is providing this notice now to help individuals understand what happened, let them know that their information may have been impacted, and give them information on steps they can take to protect their privacy, including enrolling in two years of complimentary credit monitoring and identity theft protection services if they believe that their information may have been impacted.

This substitute notice contains the information CHC can provide at this time while CHC continues working through data review to identify affected individuals. CHC plans to mail written letters on a rolling basis to affected individuals for whom CHC has a sufficient address, including on behalf of impacted customers who have been notified and who have delegated the notification process to CHC. Please note, we may not have sufficient addresses for all affected individuals. The mailing process began in late July and continues as CHC completes quality assurance procedures. Data review is ongoing, and impacted customers with attributed individuals will be notified to confirm whether they want CHC to handle notifications on their behalf. Notices were sent to impacted customers on June 20, 2024 and August 8, 2024.

What happened?

On February 21, 2024, CHC became aware of deployment of ransomware in its computer system. Once discovered, CHC quickly took steps to stop the activity, disconnected and turned off systems to prevent further impact, began an investigation, and contacted law enforcement. CHC's security team worked around the clock with several top security experts to address the matter and understand what happened. CHC has not identified evidence this incident spread beyond CHC.

CHC retained leading cybersecurity and data analysis experts to assist in the investigation, which began on February 21, 2024. On March 7, 2024, CHC was able to confirm that a substantial quantity of data had been exfiltrated from its environment between February 17, 2024, and February 20, 2024. On March 13, 2024, CHC obtained a dataset of exfiltrated files that was safe to investigate. On April 22, 2024, following analysis, CHC publicly confirmed the impacted data could cover a substantial proportion of people in America.

Although the data review is in its late stages and additional customers may be identified as impacted, CHC has identified certain customers whose members' or patients' data was involved in the incident. On June 20, 2024, CHC began providing notice to those customers on a rolling basis. In addition, CHC has provided a link to this substitute notice more generally so that other customers can provide information to their patients/members even if they have not been identified as impacted.

What information was involved?

While CHC cannot confirm exactly what data has been affected for each impacted individual, information involved for affected individuals may have included contact information (such as first and last name, address, date of birth, phone number, and email) and one or more of the following:

- Health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment);

- Billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and/or
- Other personal information such as Social Security numbers, driver's licenses or state ID numbers, or passport numbers.

The information that may have been involved will not be the same for every impacted individual. To date, we have not yet seen full medical histories appear in the data review. Also, some of this information may have related to guarantors who paid bills for health care services. A guarantor is the person who paid the bill for health care services.

Why did this happen?

A cybercriminal gained unauthorized access to the CHC computer system.

What is CHC doing?

Privacy and security are our priorities. When CHC learned about the activity, CHC immediately began an investigation with support from leading cybersecurity experts and law enforcement. In response to this incident, CHC immediately took action to shut down systems and sever connectivity to prevent further impact. CHC has also reinforced its policies and practices and implemented additional safeguards in an effort to prevent similar incidents from occurring in the future. CHC, along with leading external industry experts, continues to monitor the internet and dark web.

CHC is also sharing this website link (called a substitute notice) with additional resources in the Reference Guide for any individual who believes they may be impacted or who may have questions. The link is **https://www.changehealthcare.com/hipaa-substitute-notice**.

What individuals can do?

While CHC is still investigating whose personal information may have been involved, there are steps individuals can take to protect themselves:

- Any individual who believes their information may have been impacted by this incident can enroll in two years of complimentary credit monitoring and identity protection services. CHC is paying for the cost of these services for two years.
- Individuals should be on the lookout and regularly monitor the explanation of benefits statements received from their health plan and statements from health care providers, as well as bank and credit card statements, credit reports, and tax returns, to check for any unfamiliar activity.
- If individuals notice any health care services they did not receive listed on an explanation of benefits statement, they should contact their health plan or doctor.
- If individuals notice any suspicious activity on bank or credit card statements or on tax returns, they should immediately contact their financial institution and/or credit card company or relevant agency.
- If an individual believes they are the victim of a crime, they can contact local law enforcement authorities and file a police report.

Individuals may have additional rights available to them depending on the state they live in and should refer to the Reference Guide for additional information.

For more information

As CHC continues to work with leading industry experts to analyze data involved in this cyberattack, immediate support and robust protections are available to individuals who may be concerned about their information.

CHC regrets any inconvenience or concern caused by this incident. CHC has established a dedicated call center to offer additional resources and information to people who believe they may have been affected by this incident. Individuals can visit **changecybersupport.com** for more information and details on these resources or call the toll-free call center, which also includes trained clinicians to provide support services. The call center's number is: 1-866-262-5342, available Monday through Friday, 8 a.m. to 8 p.m. CT.

##

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 contact information below:

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
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742

TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289

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	1-800-685-1111

	Atlanta, GA 30348	
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872

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 after receiving a request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.