Notice Of Change Healthcare Cyberattack

On November 21,2024, Erie County Medical Center Corporation ("ECMCC") received formal notification from Change Healthcare ("CHC"), that ECMCC data had been compromised stemming from the ransomware attack on CHC in February 2024. CHC is a vendor that provides revenue and payment cycle management services to ECMCC. Upon learning of this event, we promptly began an investigation and have been working with CHC to understand what happened and to work to protect the privacy and security of our patients' information. While we have no indication that anyone's information has been misused, this notice describes the incident, shares information about CHC's response and outlines the measures taken in response and the steps that you can take.

For more information about this incident and CHC's response, please see CHC's notice regarding this incident on its website: **https://www.changehealthcare.com/hipaa-substitute-notice .**

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 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 CHC 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://changehealthcare.optum.com/en/hipaa-substitute-notice.html.

What all potentially affected individuals can do?
While ECMCC and CHC are 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.