LIBERTY DENTAL PLAN

Substitute Notice

On February 21, 2024, Change Healthcare became aware of deployment of ransomware in its computer system. They quickly disconnected and shut down systems to prevent further impact. An investigation was launched, and law enforcement was notified. Their security team, alongside top security experts, worked around the clock to address the issue and understand the situation. Change Healthcare has found no evidence that the event extended beyond Change Healthcare.

Change Healthcare retained leading cybersecurity and data analysis experts to help with the investigation which began on February 21, 2024. On March 7, 2024, they confirmed that a large amount of data had been exfiltrated from their systems between February 17 and February 20, 2024. On March 13, 2024, they obtained a dataset of the exfiltrated files. These files were safe to analyze and began their initial targeted analysis. On April 22, 2024, after completing the analysis, Change Healthcare publicly announced that the impacted data could affect a big portion of the American population.

On June 20, 2024, Change Healthcare began notifying customers. They also provided a link to a general substitute notice. On or after March 13, 2025, Change Healthcare informed us that some members covered by Liberty Dental Plan were among those impacted.

What information was involved?

The information that may have been involved will not be the same for every potentially impacted individual. All Change Healthcare notice letters describe the information potentially involved. Some data elements may not impact the recipient. The information involved for individuals may have included contact information (such as first and last name, address, phone number, and email), date of birth, 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 information); and/or
- Billing and claims information (such as claim numbers, account numbers, billing codes, payments made, and balance due).

What can individuals do?

Even though financial and banking information and payment cards were not impacted in this event, here are steps individuals can take to protect themselves:

- Any individual who believes their information may have been impacted by this event can enroll in two years of complimentary credit monitoring and identity protection services. Change Healthcare 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 unknown 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.

For more information

For more information about this event and to learn about services being offered to help impacted individuals protect their information, please visit https://www.changehealthcare.com/hipaa-substitute-notice.html or call Change Healthcare's support center at 1-866-262-5342 available Monday through Friday 8 a.m. to 8 p.m. CT.