CHANGE HEALTHCARE
Part of Optum

View in Browser

This communication is to inform Change Healthcare, Inc. (“CHC”) customers regarding the criminal cyberattack on CHC’s systems that included the deployment of ransomware on CHC’s systems on February 21, 2024, and provide an update on the impacted data review process undertaken by CHC.

We are in the late stages of the review of impacted data containing protected health information (PHI). **To date, we have not identified specific individuals whose PHI was impacted and who are attributed to you as a customer of CHC.** We will notify you if the final stages of the data review identify individuals whose PHI is impacted and are attributed to you.

We are separately notifying those customers for whom the review has attributed specific individuals’ PHI to the customer as the covered entity or business associate. We are providing to those customers a substitute notice they should post on the home page of their website if they wish to do so. For your information, that substitute notice is located at https://www.changehealthcare.com/hipaa-substitute-notice.

If helpful for individuals you serve, you may also post the link to the substitute notice on your website. The notice helps individuals understand what happened and gives them information on steps they can take to help protect their privacy, including enrolling in two years of complimentary credit monitoring and identity theft protection services if they are concerned their information may have been impacted. 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. – 8 p.m. CT.

CHC plans to send direct notice (written letters), based on data review, to affected individuals for whom CHC has a sufficient address. Please note we may not have sufficient addresses for all affected individuals. The mailing process is expected to begin in late July as CHC completes quality assurance procedures.

What should I do?
To date, we have not identified PHI of specific individuals that is attributable to you as a customer. This does not require any action from you — although, as outlined above, CHC has made available information and resources for individuals to help protect their privacy if (at your discretion) you think it would be helpful to make this information available by publishing the link on your website.

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.

How was my data affected?
To date, we have not identified PHI of individuals that is attributable to you as a customer. We are in the late stages of our review.

Does this mean none of my organization's information was involved in this incident? Am I in the clear?
Because the data review is in its late stages and has not yet been completed, we are not in a position to be able to make that determination. We will notify you if the final stages of the data review identify individuals whose PHI is impacted and are attributed to you.

Despite reasonable best efforts, we anticipate there will be a subset of individuals for whom we are unable to attribute to an organization as a covered entity or business associate. Change Healthcare plans to handle those HIPAA and state data breach notifications directly by mailing notice letters to those impacted individuals for whom it has a sufficient address, so they will receive notice even though we cannot identify that covered entity or business associate relationship.

When will we know with certainty whether my patients'/members' data was involved?
Once the data review is complete, we will have determined whether or not individuals with PHI impacted were attributed to your organization as a covered entity or business associate.

We continue to dedicate significant resources to analyze the data and identify individuals, their PHI and their covered entity or business associate relationships. At this point, we believe the mailing process is expected to begin in late July as CHC completes quality assurance procedures.

If I am later determined through data review to be an impacted customer, how will I know and will Change Healthcare handle

notifications on my behalf?
We will notify you if the final stages of the data review identify individuals whose PHI is impacted and are attributed to you. If and to the extent you are sent such a notice, it will explain that CHC is offering to handle notifications under HIPAA and state data breach notification laws through an opt-out process.

What patient or member PHI was potentially impacted for other customers so far?
CHC has provided details as part of the substitute notice located at https://www.changehealthcare.com/hipaa-substitute-notice.

What has Change Healthcare done about it?
CHC worked around the clock from the day of the ransomware deployment and has devoted significant resources to the response and restoration efforts, as well as retained several leading forensic firms to assist in analyzing the impacted data. However, rather than waiting to complete this review, CHC is providing free credit monitoring and identity theft protection services for two years to any U.S. individual who is concerned they may have been impacted, along with a dedicated call center staffed by clinicians to provide additional support services. Individuals may also visit changecybersupport.com for more information.

Privacy and security are our top priorities. 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.

On June 20, 2024, CHC began providing notice to customers for whom the data review has attributed specific individuals' PHI to that customer as the covered entity or business associate. CHC is taking additional steps to comply with legal obligations in relation to this incident as well as reduce the burden on its customers. These steps include notifying impacted

customers and providing substitute notice information more broadly, including to customers who have not been identified as impacted thus far. CHC will also handle HIPAA and state data breach notifications directly by mailing notice letters to those impacted individuals for whom it has a sufficient address on behalf of the impacted covered entity — unless an impacted customer opts out of the CHC notice process.

What if I have additional questions?

CHC regrets any inconvenience or concern caused by this incident. CHC values your partnership and will take steps to both mitigate the impact of this incident and prevent future security incidents from occurring in the future. Please don't hesitate to reach out to your client manager with questions. If you don't have an account representative, please go to changehealthcarecyberresponse.com and click on the data notifications inquiry button. Fill out the form to be connected to support.

Thank you for your support as this matter is resolved.

Sincerely,

The Change Healthcare Privacy Team