000042

CHANGE HEALTHCARE

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

000042

OrthoConnecticut
ATTN: Legal or Privacy Office
2 Riverview Dr
Danbury, CT 06810-6268

November 21, 2024

Change Healthcare Notice to Impacted Customers:
Substitute Notice Only - Under 500 Total Impacted Individuals

This communication is from Change Healthcare, Inc. ("CHC") to customers regarding a security incident that may have impacted your patients' or members' protected health information (PHI) that we process on your behalf. Change Healthcare is providing this notice to you pursuant to our obligations as a business associate and/or subcontractor business associate, including under the Health Insurance Portability and Accountability Act and its implementing regulations ("HIPAA"). If you received an email on June 20, 2024, indicating CHC had not identified you as a customer of CHC whose patients' or members' data was involved in the security incident thus far, this letter provides an update on our data review, through which we have now identified fewer than 500 individuals whose data was affected and who are attributed to your organization.

Based on the data review, CHC has identified not more than 103 patients or members whose data was involved in the security incident and attributed to Danbury Orthopedic Associates. **Notwithstanding, we do not have sufficient address information to send notice letters to any of your impacted patients/members.**

- If you are a HIPAA covered entity, the next step is for you to post a HIPAA substitute notice link on your website for individuals to see. Instructions are included on the next page. Unless you opt out as outlined below by December 3, 2024, CHC will handle legally required notification on your behalf to the U.S. Department of Health & Human Services Office for Civil Rights (OCR), provide a HIPAA substitute notice for you to post, and media notice under HIPAA as required; **no further action is required by you**.
- If you are a HIPAA business associate which uses CHC to help provide services to your own covered entity customers, this security incident may have impacted your customers' PHI. You may wish to forward this notice to those covered entity customers for their review and action, as detailed on the next page.

Please note that you may receive both an email and a mailing with this information. We encourage you to forward the information to your privacy office for your records.

What should I do?
Substitute Notice. CHC is providing a HIPAA substitute notice link you should prominently post on the home page of your website now for at least 90 consecutive days. That link is https://www.changehealthcare.com/hipaa-substitute-notice. Consistent with HIPAA, substitute notice is an alternative to individual notice letters if there is insufficient address information for 10 or more individuals. Accordingly, the notice includes a description of information which may have been involved, a toll-free call center number for individuals, and information on complimentary credit monitoring and identity protection services available to individuals now if they are concerned they may have been impacted.

Notice To OCR and HIPAA Media Notice To Be Handled by CHC, Unless Covered Entities Opt Out. If you are a HIPAA covered entity customer, CHC will handle notifying OCR and providing media notice under HIPAA as required by law on your behalf as a delegate, unless you decide to opt out in writing by sending an email to chc_cyber_event_customer_inquiry@optum.com by **December 3, 2024**. If you opt out, this means that you will handle your own notifications under HIPAA. If you opt out of CHC's notification process, you cannot opt back in. **You do not need to do anything to opt in, and we will proceed on your behalf unless you opt out.**

Opt-Out Process to Handle Your Own Notices; Specific Deadline to Opt Out. If you choose to opt out, CHC will provide data for you to validate your members/patients and you will be responsible for locating their addresses and sending notifications to your impacted members/patients under HIPAA and state law, as well as posting any substitute notice and media notice as appropriate. This is a one-time opt-out process. If you wish to opt out of CHC's notification process, please send an email to chc_cyber_event_customer_inquiry@optum.com by **December 3, 2024**. Once you opt out, you cannot opt back into the CHC notification process. If we have not received an opt-out request by **December 3, 2024,** we will proceed with satisfying the notification on your behalf.

If you are a HIPAA business associate which uses CHC to help provide services to your own covered entity customers, you may wish to **forward this notice** to those covered entity customers for their review and action, including the decision to handle their own notification to OCR, HIPAA substitute notice, and media notice under HIPAA, as appropriate. CHC will proceed as a delegate to notify OCR on your covered entity customers' behalf, unless your covered entity customer sends an email to chc_cyber_event_customer_inquiry@optum.com by **December 3, 2024** and expresses their wish to opt out of that notification. If your covered entity customer opts out, this means that the customer will handle their own notification to OCR. If a covered entity opts out of CHC's notification process, they cannot opt back in.

Please find below additional information about the CHC incident:

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 further analysis, CHC confirmed that the impacted data was likely to affect a substantial proportion of people in America.

How was my data affected?
CHC conducted an extensive review of the data to identify specific covered entities and specific individuals impacted by this security incident. Based on the data review, CHC has determined that your patients' or members' PHI has been affected by the incident.

What patient or member PHI/PII was potentially impacted?
While CHC cannot confirm exactly what data has been affected for each specific individual, based on its review, information involved for your affected patients and members may have included contact information (such as first and last name, 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 was not the same for every impacted individual. Also, some of this information may have related to guarantors who paid bills for health care services.

Here are some steps individuals can take to protect themselves:

- Any individual concerned that 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.

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 expert forensic firms to analyze the impacted data. However, rather than waiting to complete this review, CHC has already been 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 https://www.unitedhealthgroup.com/changehealthcarecyberresponse for more information.

Privacy and security are our 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 evaluated additional safeguards in an effort to prevent similar incidents from occurring in the future. Change Healthcare, along with leading external industry experts, continues to monitor the internet and dark web.

On June 20, 2024, CHC began providing notice to customers for whom the data review has matched specific individuals' PHI to that customer as the covered entity or business associate. CHC is committed to compliance with legal obligations in relation to this incident as well as reducing the burden on its customers. CHC has also been in ongoing discussions with the OCR regarding this incident.

What if I have a question?
CHC has established a dedicated customer call center to offer additional resources and information regarding the incident. If you have any questions or concerns, please call us toll-free at 1-866-674-1298, available Monday through Friday, 8 a.m. to 8 p.m. CT.

CHC regrets any inconvenience or concern caused by this incident, and we value your partnership.

Thank you for your support as this matter is resolved.

Sincerely,

Mitchell W. Granberg

Mitch Granberg
Chief Privacy Officer