



CHANGE HEALTHCARE

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



CONCORD OPHTHALMOLOGIC ASSOCI
CONCORD EYE CENTER
2 PILLSBURY ST STE 100
CONCORD, NH 03301-3549



September 16, 2024

Notice of Security Incident

To: CONCORD OPHTHALMOLOGIC ASSOCI

You are receiving this notice from Change Healthcare, Inc. (“CHC”). CHC provides services on behalf of Veradigm LLC (previously known as AllScripts) to you or your organization. As discussed in more detail below, CHC experienced a security incident that impacted protected health information. CHC has identified you as a Veradigm customer whose patients’ or members’ data was involved in the security incident. CHC is providing the information below to assist in preparations for any legally required notifications to individuals, the U.S. Department of Health & Human Services, the Office for Civil Rights (“OCR”) and state attorneys general while CHC completes its data analysis. Unless you opt out as outlined below, CHC will provide the notifications specified below on your behalf.

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. If you want CHC to handle HIPAA and state data breach notices on your behalf, you do not need to take further action – please post the HIPAA substitute notice link on your website, if you have a website. This link is provided below.

If you are a HIPAA covered entity, please review this notice carefully:

- 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>. This substitute notice contains the information CHC can provide at this time while CHC continues working through data review to identify affected individuals. This includes a description of information which may have been involved based on review to date, a toll-free call center number, and information on complimentary credit monitoring and identity protection services available to individuals now if they are concerned they may have been impacted.
- 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 already underway.
- **CHC’s notification process is an opt-out process. If you wish to opt out, please send an email to chc_cyber_event_allscripts_customers@optum.com by September 30, 2024.** If you, as a covered entity, do not opt out, you **do not need to contact us** and CHC will proceed as a delegate on your behalf to provide the following notifications:

- HIPAA substitute notice
- HIPAA media notice
- OCR report, when data review is completed
- Individual notifications under HIPAA and state law, for impacted individuals with sufficient address information
- Notice to state attorneys general as appropriate
- Impacted individuals with an unknown or insufficient address will be provided notice via substitute notice.
- **If you opt out of CHC's notification process, you cannot opt back in.**

What should I do?

Substitute Notice. CHC is providing a HIPAA substitute notice, <https://www.changehealthcare.com/hipaa-substitute-notice>, which should be posted prominently on covered entities' home pages for at least 90 consecutive days, in compliance with HIPAA substitute notice requirements. While CHC is still reviewing the data, covered entities should provide patients/members with information via the substitute notice link available to you now.

Notices To Be Handled by CHC, Unless Covered Entities Opt Out. If you are a HIPAA covered entity customer, CHC is offering to make HIPAA and state attorney general notifications as required by state law on your behalf as a delegate, unless you decide to opt out of CHC's notification process and handle your own notices. CHC's substitute notice under HIPAA, notice letters to affected individuals, media notice under HIPAA, and OCR and state attorney general notice filing will be on behalf of impacted CHC covered entity customers, except for those customers who opt out to handle their own notifications. **If you want CHC to manage these notifications for you, you do not need to respond.** You do not need to do anything to opt in, and if you do not opt out, we will proceed on your behalf.

Opt-Out Process to Handle Your Own Notices; Specific Deadline to Opt Out. You can choose to issue your own notifications if that is your preference by opting out of CHC's notification process. If you choose to opt out, when the data analysis is complete, CHC will provide data for you to validate your members/patients and you will be responsible for validating their addresses and sending notifications to your impacted members/patients under HIPAA and state law. This is a one-time opt-out process. If you wish to opt out of CHC's notification process, please notify chc_cyber_event_allscripts_customers@optum.com by **September 30, 2024**. Once you opt out, you cannot opt back into the CHC notification process. If we have not received an opt-out request by **September 30, 2024**, we will proceed with satisfying the notification on your behalf.

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?

At this time, data review is in its late stages to identify specific covered entities and specific individuals impacted by this security incident. However, based on the data review thus far, 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 to date, information involved for your affected patients and members 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 was not the same for every impacted individual. To date, CHC has 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.

While CHC is still investigating whose personal information may have been involved, there 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 begun 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 been in ongoing discussions with the OCR regarding this incident. While substitute notice was discussed with the OCR, the OCR also emphasized the need for individual letters to be sent directly. To reduce the burden on impacted customers, CHC will validate addresses and will draft and send direct notice letters as required to those individuals identified through data review attributable to specific customers and for whom CHC has sufficient addresses, on behalf of impacted covered entity customers — *unless* those customers opt out by the specific deadline.

What if I have a question?

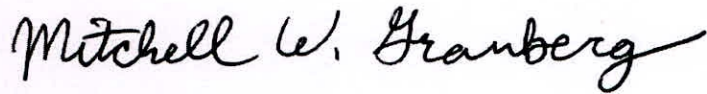
CHC has established a dedicated Veradigm customer call center to offer additional resources and information regarding the incident. If you have any questions or concerns, please call us toll-free at 1-866-814-7264, available Monday through Friday, 8 a.m. to 8 p.m. CT.

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

Please do not hesitate to contact us by going to <https://www.unitedhealthgroup.com/changehealthcarecyberresponse> and clicking 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,

A handwritten signature in black ink that reads "Mitchell W. Granberg". The signature is written in a cursive style with a long, sweeping underline.

Mitch Granberg
Chief Privacy Officer