# What You Should Know

Last Modified on 07/12/2024 11:42 am EDT

At this time, Change Healthcare (CHC) is continuing its investigation into the February 21st cyberattack and has not completed its analysis of the impacted customer's data. Given the ongoing nature and complexity of the data review, it will require several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals.

As CHC continues to work with leading industry experts to analyze data involved in this cyberattack, it is immediately providing support and robust protections rather than waiting until the conclusion of the data review. You can visit the CHC-dedicated website **https://www.unitedhealthgroup.com/ns/health-data-breach.html** to obtain more information and details on available resources.

In addition, CHC has established a dedicated call center to offer free credit monitoring and identity theft protection for two years to anyone impacted. The call center includes trained clinicians to provide support services. Given the ongoing nature and complexity of the data review, the call center will not be able to provide any specifics on individual data impact at this time. The call center can be reached at **1-866-262-5342** and further details can be found on the website.

Upon completion of their investigation, UnitedHealth Group (UNH) will help ease reporting obligations on other stakeholders whose data may have been compromised as part of the CHC cyberattack. UNH has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer if their data is found to be compromised. Notifications will be made efficiently and in compliance with legal requirements, including direct mail, website notices, and other necessary communications.

Protecting your personal health information is—and always will be—one of our top priorities. We will continue to monitor the UNH/CHC investigation closely and provide updates to our valued customers as additional information becomes available.

**Additional References**:

The U.S. Department of Health and Human Services Office for Civil Rights published a dedicated website (https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html) to share answers to frequently asked questions concerning Health Insurance Portability and Accountability Act rules and the cybersecurity attack.

The Federal Trade Commission also offers resources to help protect your identity. For additional information about other precautions available to you, visit the Federal Trade Commission website (http://www.consumer.ftc.gov/features/feature-0014-identity-theft).

Please look at our **ePS Affected/Reconnected Payer Routes** lists below. **Note**: We will post regular updates to the lists as they become available.