

UnitedHealth says wide swath of patient files may have been taken in Change cyberattack

April 23 2024, by Tom Murphy



Pages from the United Healthcare website are displayed on a computer screen, Feb. 29, 2024, in New York. UnitedHealth says files with personal information that could cover “a substantial portion of people in America” may have been taken in the cyberattack on its Change Healthcare business. The company said Monday, April 22, 2024 after markets closed that it sees no signs that doctor charts or full medical histories were released after the attack. Credit: AP Photo/Patrick Sison, File

UnitedHealth says files with personal information that could cover a "substantial portion of people in America" may have been taken in [the cyberattack](#) earlier this year on its Change Healthcare business.

The company said Monday after markets closed that it sees no signs that doctor charts or full medical histories were released after the attack. But it may take several months of analysis before UnitedHealth can identify and notify people who were affected.

UnitedHealth did say that some screen shots containing protected health information or personally identifiable information were posted for about a week online on the dark web, which standard browsers can't access.

The company is still monitoring the internet and [dark web](#) and said there has been no additional file publication. It has started [a website](#) to answer questions and a call center. But the company said it won't be able to offer specifics on the impact to individual data.

The company also is offering free credit monitoring and identity theft protection for people affected by the attack.

UnitedHealth bought Change Healthcare in a roughly \$8 billion deal that closed in 2022 after surviving a challenge from [federal regulators](#). The U.S. Department of Justice had sued earlier that year to block the deal, arguing that it would hurt competition by putting too much information about health care claims in the hands of one company.

UnitedHealth said in February that a ransomware group had gained access to some of the systems of its Change Healthcare business, which provides technology used to submit and process insurance claims.

The attack disrupted payment and claims processing around the country, stressing doctor's offices and health care systems.

[Federal civil rights investigators](#) are already looking into whether protected [health information](#) was exposed in the attack.

UnitedHealth said Monday that it was still restoring services disrupted by the attack. It has been focused first on restoring those that affect patient access to care or medication.

The company said both pharmacy services and medical claims were back to near normal levels. It said payment process was back to about 86% of pre-attack levels.

UnitedHealth said last week when it reported [first-quarter](#) results that the company has provided more than \$6 billion in advance funding and interest-free loans to health care providers affected by the attack.

UnitedHealth took an \$872 million hit from from the cyberattack in the first quarter, and company officials said that could grow beyond \$1.5 billion for the year.

Minnetonka, Minnesota-based UnitedHealth Group Inc. runs one of the nation's largest health insurers. It also runs one of the nation's largest pharmacy benefits management businesses, provides care and offers technology services.

Company slipped nearly \$3 to \$488.36 in midday trading Tuesday while broader indexes climbed.

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: UnitedHealth says wide swath of patient files may have been taken in Change

cyberattack (2024, April 23) retrieved 4 May 2024 from
<https://techxplore.com/news/2024-04-unitedhealth-wide-swath-patient-cyberattack.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.