Cencora confirms patient health info stolen in February attack

By
Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)

August 1, 2024 12:30 PM **0**

Pharmaceutical giant Cencora has confirmed that patients' protected health information and personally identifiable information (PII) was exposed in a February cyberattack.

Cencora, previously known as AmerisourceBergen, specializes in pharmaceutical services, providing drug distribution and technology solutions for doctor's offices, pharmacies, and animal healthcare.

The company is ranked #10 on the Fortune 500 and #24 on the Global Fortune 500, with a revenue of more than $250 billion.

When Cencora first disclosed the cyberattack (https://www.bleepingcomputer.com/news/security/pharmaceutical-giant-cencora-says-data-was-stolen-in-a-cyberattack/) in February, it warned that the threat actors had stolen personal information.

In a Wednesday FORM 8-K filing with the SEC, Cencora has now confirmed that protected health information and personally identifiable information were also stolen.

"Through that investigation, the Company learned that additional data, beyond what was initially identified, had been exfiltrated. The Company has identified and completed its review of most of the exfiltrated data (the "Data")," reads the SEC filing (https://www.sec.gov/Archives/edgar/data/1140859/000110465924084351/tm2420501d1_8ka.htm).

"This review has confirmed that the Data included personally identifiable information ("PII") and protected health information ("PHI") of individuals, most of which is maintained by a Company subsidiary that provides patient support services."

This is the first time that Cencora confirmed protected health information was exposed. However, some of the largest pharmaceutical firms in the United States that partner with Cencora had already disclosed that patient's health information was exposed (https://www.bleepingcomputer.com/news/security/cencora-data-breach-exposes-us-patient-info-from-11-drug-companies/) in the attack.

This information includes a patient's first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions.

Some of the pharmaceutical companies impacted by this breach include Novartis, Bayer, AbbVie, Regeneron Pharmaceuticals, Genentech, Incyte, Sumitomo Pharma America, Acadia Pharmaceuticals, GlaxoSmithKline Group, Endo Pharmaceuticals, and Dendreon Pharmaceuticals.

Cencora has not shared much information about the cyberattack other than telling BleepingComputer that they did not believe there was a connection between their incident and the Change Healthcare attack.

Recently, it was revealed that a Fortune 50 company paid a record-breaking $75 million ransom (https://www.bleepingcomputer.com/news/security/dark-angels-ransomware-receives-record-breaking-75-million-ransom/) to the Dark Angels ransomware operation early this year.

While Cencora has not confirmed whether it suffered a ransomware attack or paid a ransom, it is the only Fortune 50 company known to have suffered a cyberattack that was not claimed by a threat actor.

BleepingComputer contacted Cencora earlier this week to ask if they paid a ransom but did not receive a response.

Related Articles:

Columbus investigates whether data was stolen in ransomware attack (https://www.bleepingcomputer.com/news/security/columbus-investigates-whether-data-was-stolen-in-ransomware-attack/)

AMD investigates breach after data for sale on hacking forum (https://www.bleepingcomputer.com/news/security/amd-investigates-breach-after-data-for-sale-on-hacking-forum/)

Keytronic confirms data breach after ransomware gang leaks stolen files (https://www.bleepingcomputer.com/news/security/keytronic-confirms-data-breach-after-ransomware-gang-leaks-stolen-files/)

World leading silver producer Fresnillo discloses cyberattack (https://www.bleepingcomputer.com/news/security/world-leading-silver-producer-fresnillo-discloses-cyberattack/)

Hot topics: Can’t-miss sessions at Mandiant’s 2024 mWISE event (https://www.bleepingcomputer.com/news/security/hot-topics-cant-miss-sessions-at-mandiants-2024-mwise-event/)

CENCORA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CENCORA/)

CYBERATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBERATTACK/)

DATA THEFT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DATA-THEFT/)

PERSONALLY IDENTIFIABLE INFORMATION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PERSONALLY-IDENTIFIABLE-INFORMATION/)

PHARMACEUTICAL (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHARMACEUTICAL/)

PII (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PII/)

PROTECTED HEALTH INFORMATION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PROTECTED-HEALTH-INFORMATION/)

(https://www.bleepingcomputer.com/author/lawrence-abrams/)

LAWRENCE ABRAMS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/LAWRENCE-ABRAMS/)

(MAILTO:LAWRENCE.ABRAMS@BLEEPINGCOMPUTER.COM) (HTTPS://TWITTER.COM/LAWRENCEABRAMS)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/SITE-WARNS-OF-SCAMMERS-POSING-AS-CRYPTO-EXCHANGE-EMPLOYEES/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/SITE-DUCKS-DNS-ATTACKS-LET-HACKERS-HIJACK-OVER-35-000-DOMAINS/)

POPULAR STORIES

Microsoft says massive Azure outage was caused by DDoS attack

(https://www.bleepingcomputer.com/news/microsoft/microsoft-says-massive-azure-outage-was-caused-by-ddos-attack/)

New Android malware wipes your device after draining bank accounts

(https://www.bleepingcomputer.com/news/security/new-android-malware-wipes-your-device-after-draining-bank-accounts/)

FOLLOW US:

(https://www.bleepingcomputer.com)

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

VPN Buyer Guides (https://www.bleepingcomputer.com/vpn/)

SysAdmin Software Guides (https://www.bleepingcomputer.com/sysadmin/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)