

Cencora data breach exposes US patient info from 11 drug companies

By **Bill Toulas**



May 24, 2024



11:44 AM



2



cencora

Post updated on 5/25 to add three more pharmaceutical firms also impacted by the Cencora security breach.

Some of the largest drug companies in the world have disclosed data breaches due to a February 2024 cyberattack at Cencora, whom they partner with for pharmaceutical and business services.

Cencora, formerly AmerisourceBergen, is a pharmaceutical services provider specializing in drug distribution, specialty pharmacy, consulting, and clinical trial support.

The Pennsylvania-based firm, with a presence in 50 countries, employs 46,000 people and has a revenue (2023) of \$262 billion.

In February 2024, Cencora [disclosed a data breach](#) in a Form 8-K filing with the SEC, stating that unauthorized parties gained access to its information systems and exfiltrated personal data.

At the time, the company opted not to share any additional information regarding the incident and its potential impact on its clients. Also, no ransomware groups ever assumed responsibility for the attack.

Today, the California Attorney General's office published multiple data breach notification samples submitted in the past couple of days by some of the largest pharmaceutical firms in the United States, all attributing their data exposure to the February Cencora incident.

"Cencora, Inc. and its Lash Group affiliate partner with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to prescribed therapies through drug distribution, free trial offers, co-pay coupons, patient support and services, and other services," reads a related data breach notification from Novartis.

"We take the privacy and protection of the information entrusted to us very seriously. Cencora is writing to let you know about an event that involved your personal information that Cencora maintains in connection with its patient support programs on behalf of Novartis Pharmaceuticals Corporation."

The eleven firms impacted by this breach, all using almost identical data breach notifications, are:

1. **Novartis Pharmaceuticals Corporation** – One of the largest pharmaceutical companies globally, with a strong presence in various therapeutic areas including oncology, neuroscience, and immunology.
2. **Bayer Corporation** – A large multinational company with significant operations in pharmaceuticals, consumer health, and agricultural products.
3. **AbbVie Inc.** – Known for its blockbuster drug Humira, AbbVie is a major player in immunology and oncology.
4. **Regeneron Pharmaceuticals, Inc.** - Notable for its innovative treatments in ophthalmology, oncology, and immunology.
5. **Genentech, Inc.** – A member of the Roche Group, Genentech is a leader in biotechnology and has made significant contributions to cancer treatment.
6. **Incyte Corporation** – Focuses on oncology and hematology, with key products like Jakafi.

7. **Sumitomo Pharma America, Inc.** – Part of the Sumitomo Pharma Co., Ltd., known for its diverse portfolio in psychiatry, neurology, and oncology.
8. **Acadia Pharmaceuticals Inc.** – Specializes in central nervous system disorders and has a smaller market presence than the others in this list.
9. **GlaxoSmithKline Group** - A global healthcare company known for its wide-ranging portfolio in pharmaceuticals, vaccines, and consumer healthcare, with significant efforts in respiratory diseases, HIV, and immuno-inflammation.
10. **Endo Pharmaceuticals Inc.**- Specializes in pain management, urology, and endocrinology, with a notable presence in both branded and generic pharmaceuticals.
11. **Dendreon Pharmaceuticals LLC** - Focuses primarily on oncology, particularly in the development and commercialization of immunotherapy treatments for prostate cancer.

The data breach notices warn that Cencora's internal investigation, which concluded on April 10, 2024, confirmed that the following information had been exposed: full name, address, health diagnosis, medications, and prescriptions.

The letter notes that as of this time, there's no evidence that the exfiltrated information has been publicly disclosed on the internet or that it has been used for fraudulent purposes.

As a response to the elevated risk for exposed individuals, Cencora is offering recipients two years of free identity protection and credit monitoring services through Experian, which they can take advantage of until August 30, 2024.

BleepingComputer has reached out to Cencora to learn more about the data breach incident as well as the number of people impacted, but a spokesperson declined to provide additional details, pointing us to a [news release](#) issued last week.

AMERISOURCEBERGEN

CENCORA

CUSTOMER DATA

DATA BREACH

HEALTHCARE

PHARMACEUTICAL





BILL TOULAS

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

[< PREVIOUS ARTICLE](#)[NEXT ARTICLE >](#)

Comments



DX9895 - 2 days ago



Thanks for this article. Cencora's "disclosure" is totally opaque.
[Cencora 2023 revenue: \$262 billion. Who knew?!]



tadees - 2 days ago



Any information on how to use the free Experian service they're supposedly offering? Cencora's website is absolutely silent about this (data breach, data leak, and Experian returned no results).
Thanks.