

Johnson & Johnson discloses IBM data breach impacting patients

By Bill Toulas

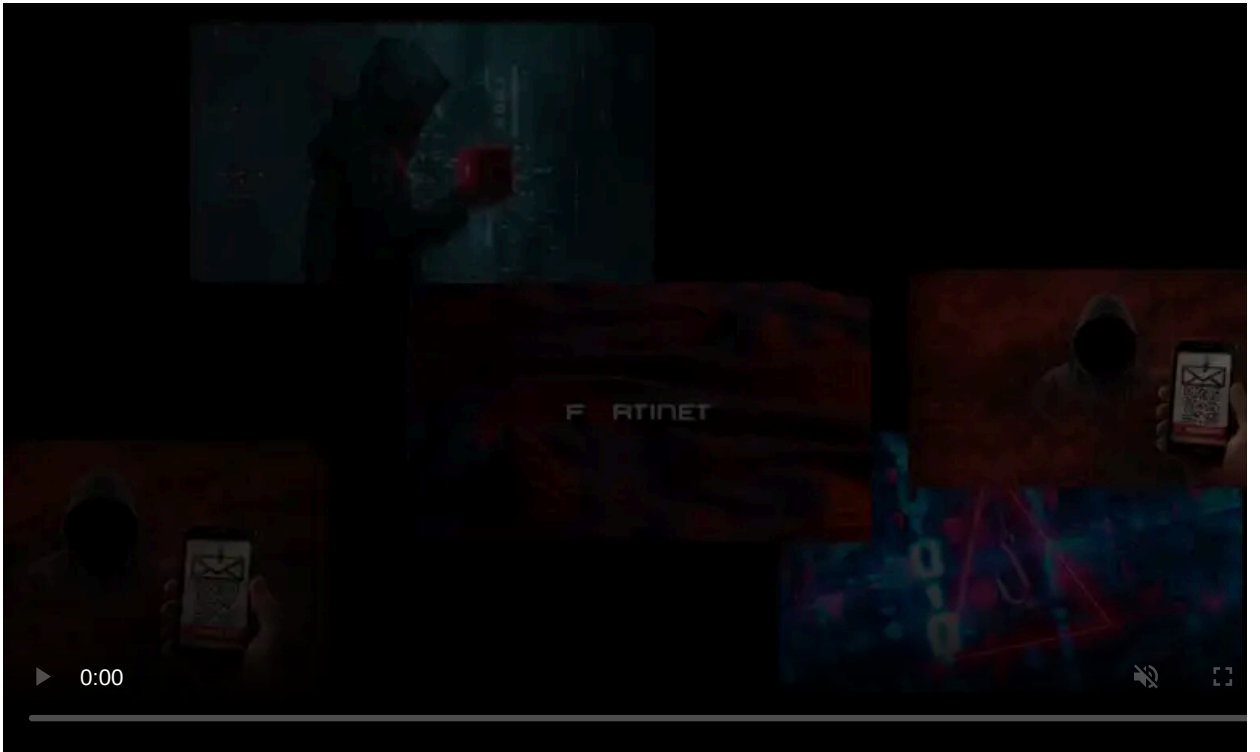
Published: 2023-09-07 · Archived: 2026-04-05 23:15:28 UTC



Johnson & Johnson Health Care Systems ("Janssen") has informed its CarePath customers that their sensitive information has been compromised in a third-party data breach involving IBM.

IBM is a technology service provider for Janssen; specifically, it manages the CarePath application and database supporting its functions.

CarePath is an application designed to help patients gain access to Janssen medications, offer discounts and cost-saving advice on eligible prescriptions, provides guidance on insurance coverage, and serves drug refiling and administering alerts.



Visit Advertiser website [GO TO PAGE](#)

According to the [notice on Janssen's site](#), the pharmaceutical firm became aware of a previously undocumented method that could give unauthorized users access to the CarePath database.

The firm reported this to IBM, who promptly fixed the security gap and launched an internal investigation to assess if anyone had exploited the flaw.

Unfortunately, the investigation that was concluded on August 2nd, 2023, showed that unauthorized users accessed the following CarePath user details:

- Full name
- Contact information
- Date of birth
- Health insurance information
- Medication information
- Medical condition information

The exposure impacts CarePath users who enrolled on Janssen's online services before July 2nd, 2023, which might indicate that the breach occurred on that date or the breached database was a backup.

Social security numbers and financial account data were not kept in the breached database, so those critical details have not been exposed.

Also, the pharmaceutical firm has clarified that this security incident doesn't impact Janssen's Pulmonary Hypertension patients.

The compromised data could support highly effective phishing, scamming, and social engineering attacks, and considering the value of medical data, there is a high chance they will be sold for a premium on darknet markets.

IBM has [published a separate announcement](#) about the incident that says there are no indications the stolen data has been misused. Still, IBM urges Janssen CarePath users to remain vigilant and closely monitor their account statements for suspicious activity.

Also, the tech giant is now offering a one-year credit monitoring free of charge to all impacted individuals to help protect them from fraud.

Both announcements share toll-free numbers where providers and users may call to address their questions about the incident or get help enrolling in credit monitoring services.

IBM is also among the hundreds of entities breached by Clop ransomware earlier this year when the notorious threat actors exploited a [zero-day vulnerability on the MOVEit Transfer](#) software used by numerous organizations worldwide.

A couple of weeks back, the Colorado Department of Health Care Policy & Financing (HCPF) [informed four million individuals](#) that their personal and medical data had been exposed due to the breach on IBM.

BleepingComputer has asked IBM about whether this incident is related to the MOVEit attack, and a spokesperson told us that it is a separate incident caused by different threat actors.

On the question of how many people have been impacted, IBM told BleepingComputer that they are notifying all CarePath users.

Article updated to add clarifications provided by IBM regarding the attack and scope of the incident.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/johnson-and-johnson-discloses-ibm-data-breach-impacting-patients/>