Doctor Alliance Investigating 353 GB Data Theft Claim

By Steve Alder

Published: 2025-11-17 · Archived: 2026-04-05 13:25:59 UTC

Posted By on Nov 17, 2025

Dallas, TX-based Doctor Alliance, a HIPAA business associate that provides document management and billing services to HIPAA-covered entities, is investigating a claim that a hacker exfiltrated 353 GB of data in a November cyberattack.

On or around November 7, 2025, a hacker using the moniker Kazu, added a post to an underground hacking forum claiming to have stolen 1.24 million files from Doctor Alliance. The hacker has demanded a $200,000 ransom, payment of which is required to ensure that the stolen data is deleted. The hacker has threatened to sell the data if the ransom is not paid.

A 200 MB sample was added to the listing that was analyzed and found to contain what appears to be patient names, addresses, phone numbers, email addresses, medical record numbers, Medicare numbers, diagnoses, treatment information, medications, and provider information. According to the leak site, Doctor Alliance has until November 21, 2025, to pay the ransom.

While the sample appears to include patient data, it has yet to be confirmed whether the data came from Doctor Alliance. It is possible that the data came from a previous data breach at an unrelated entity. Doctor Alliance has issued a statement confirming it is aware of the claim, has engaged cybersecurity experts to determine whether its network was compromised, and is analyzing the data sample to determine if the claim is valid. Doctor Alliance has confirmed that a single client account has been accessed by an unauthorized individual, and that immediate action was taken to contain the incident. The vulnerability that was exploited was remediated on the day of discovery, but Doctor Alliance has not confirmed if data was stolen in that incident.

It is unclear whether Kazu is an individual or a member of a hacking group. The Kazu data leak site currently lists more than 30 victims from spring 2025. Other victims on the leak site include government entities, the military, and other healthcare organizations. Kazu does not appear to have previously targeted entities in the United States, appearing to favor entities in South America, Asia, and the Middle East. The dark web data leak site includes victims from Argentina, Bolivia, Colombia, Costa Rica, Iran, Mauritania, Mexico, Nepal, Saudi Arabia, Sri Lanka, Thailand, and Venezuela. Doctor Alliance is currently the only listed U.S. victim.

The lack of confirmation of data theft has not prevented legal action from being taken. Multiple class action lawsuits have already been filed in the United States District Court for the Northern District of Texas, Dallas Division, by individuals who claim to have been affected. One of those lawsuits was filed by Barbara Catabia, individually and on behalf of similarly situated individuals. According to the lawsuit, “There is no question Plaintiff’s and Class Members’ Private Information is in the hands of cybercriminals who will continue to use the stolen Private Information for nefarious purposes for the rest of their lives.”

The lawsuit claims Doctor Alliance provides services to healthcare organizations such as Intrepid, AccentCare, Interim, and Prima Care. Prima Care is also named as a defendant in the lawsuit. The lawsuit asserts claims of negligence, negligence *per se,* breach of implied contract, unjust enrichment, breach of fiduciary duty, and breach of third-party beneficiary contract. The lawsuit seeks class action certification, a jury trial, compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys’ fees and costs, and other remedies deemed appropriate by the court.
