From bad to worse: Doctor Alliance hacked again by same threat actor (2) - DataBreaches.Net

Published: 2025-11-18 · Archived: 2026-04-11 02:06:31 UTC

On November 12, DataBreaches reported that **Doctor Alliance** had allegedly been hacked by a threat actor who listed the data for sale on a clearnet forum. At the time, "Kazu" claimed to have 353 GB of data and had given Doctor Alliance a November 21 deadline to pay $200,000 or the data would be sold to others.

As previously noted, Kazu told DataBreaches that he had exploited an older vulnerability that Doctor Alliance had not patched. When emailed about his claims, a spokesperson for Doctor Alliance told DataBreaches that they were investigating the claims but had not confirmed anything. They did not respond to subsequent inquiries when DataBreaches sent them sample files and a screenshot allegedly demonstrating Kazu had access.

Although they failed to provide any further statement to DataBreaches, Doctor Alliance apparently responded to others' inquiries by acknowledging that they had recently identified unauthorized access involving a single client account. "The issue was contained immediately, impacted systems were secured and the vulnerability was corrected the same day. We are currently working with independent security experts to complete a thorough analysis of the incident. At this stage, we have not verified the claims or numbers circulating online," they informed ISMG.

Their lack of confirmation or denial did not stop personal injury law firms from seeking plaintiffs for class action litigation or from filing lawsuits already. By now, four potential class action lawsuits have been filed in federal court in the Northern District of Texas.

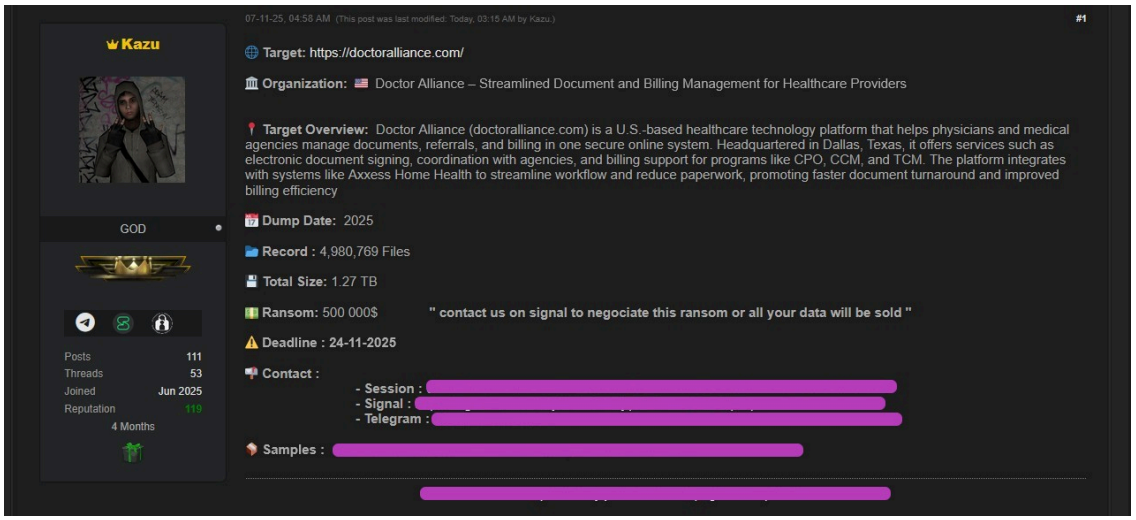
But Doctor Alliance has an even bigger problem now. It appears Kazu has hacked them again.

The Second Hack

On Kazu's Telegram channel, he wrote:

> After seeing Vivek Kushalnagar Srinivas, the CEO of Doctor Alliance, proudly announce that the company had "fixed the vulnerability" on the same day our first message was published — we decided to dig deeper.
>
> We decide to search and exploit more vulnerabilities in their system .
>
> This time, we managed to extract a total of approximately 5 million files, including:
>
> 3,740,129 signed documents from all PGs (917 GB)
>
> 1,240,640 unsigned files (353 GB)
>
> Total: nearly 1.27 terabytes of stolen data.

A check of Kazu's original forum listing shows that the listing was updated to reflect those numbers. The deadline for Doctor Alliance to respond to them has been revised to November 25, but now the amount is no longer $200,000 but $500,000, as shown below:



Updated listing by Kazu on clear net forum. Image and redaction: DataBreaches.net

In an online chat, Kazu informed DataBreaches that the second attack was launched over the past weekend when employees were not working. He reportedly tried to dump all the files in just 5-7 hours using all his servers. Doctor Alliance employees reportedly did not detect the breach until Monday. As before, Kazu emailed the firm with samples of the data he had acquired.

As far as DataBreaches knows, Doctor Alliance has not responded directly to Kazu nor attempted to negotiate either after the first attack nor this second one that Kazu claims.

DataBreaches asked Kazu whether the second attack involved the same vulnerability as the first attack. He responded that it did, and that he was able to gain access using an account with high privileges. When asked where/how he acquired the credentials, Kazu responded that Doctor Alliance reuses some admin passwords across multiple admin accounts, and he was able to find one by looking at infostealer logs. DataBreaches is unable to attempt to verify those claims.

More Than 1 Million Patients Affected?

Doctor Alliance has many clients, each with many patients. If Kazu exfiltrated more than 5 million records, even if there were many duplicates or multiple files for any one patient, this breach likely impacted a significant number of patients' sensitive protected health information and personal information.

DataBreaches did not include screenshots of purported patient records in the previous post, but because Doctor Alliance has neither confirmed nor denied that they are real, we are posting a few here to show readers what the data tranche looks like. Kazu provided DataBreaches with an expanded sample of more than 100GB of files. As before, DataBreaches was able to spot-check and find real people with the names, addresses, and dates of birth as the patient records in the tranche.

To give readers a sense of how much protected health information has been compromised, consider two redacted screenshots below. Each one represents a unique patient. The first screenshot is the first page of a multi-page .pdf record for a New Mexico patient with Stage 4 rectal cancer. In addition to her name, date of birth, address, phone number, medical record number, and information on the healthcare provider, the cover sheets lists her primary and secondary diagnoses as well as significant medical details, cognitive status, mood, and patient risk profile.

Home Health Certification and Plan of Care — Order Number [redacted] of 4

Patient Information

Patient's HI Claim No.	Start of Care Date	Certification Period	Medical Record No.
[redacted]	09/25/2024	From: 09/25/2024 To: 11/23/2024	[redacted]

Patient's Name and Address	Gender	Date of Birth	Phone Number
[redacted]	Female	[redacted]	[redacted]
	Email: --		Primary Language: English

Patient Risk Profile
Risk Factors: Multiple hospitalizations (2 or more) in the past 6 months. Multiple emergency department visits (2 or more) in the past 6 months.

Additional Risk Information: stage 4 rectal cancer

Clinical Data

Clinical Manager	Branch Name and Address	Phone Number
--	Elite Home Health, LLC. 1508 N Dal Paso Street Hobbs, NM 88240-4042	(575) 393-9281
Provider Number - Medicare Number: [redacted]		Fax Number: (575) 393-9332

Primary Diagnosis

Code	Description	Date
C20.	Malignant neoplasm of rectum (E)	09/25/2024

Secondary/Other Diagnosis

Code	Description	Date
Z43.2	Encounter for attention to ileostomy (O)	09/25/2024
C79.31	Secondary malignant neoplasm of brain (E)	09/25/2024
R47.1	Dysarthria and anarthria (E)	09/25/2024
I10.	Essential (primary) hypertension (E)	09/25/2024
E78.00	Pure hypercholesterolemia, unspecified (E)	09/25/2024
E03.9	Hypothyroidism, unspecified (E)	09/25/2024
Z86.718	Personal history of other venous thrombosis and embolism (E)	09/25/2024
Z91.81	History of falling (E)	09/25/2024

Mental Status
Orientation:
Person: Oriented. Time : Oriented.
Place : Oriented. Situation: Oriented.

Memory: No problems.

Neurological: No problems.

Mood: Appropriate (WNL).

Behavioral: Appropriate (WNL).

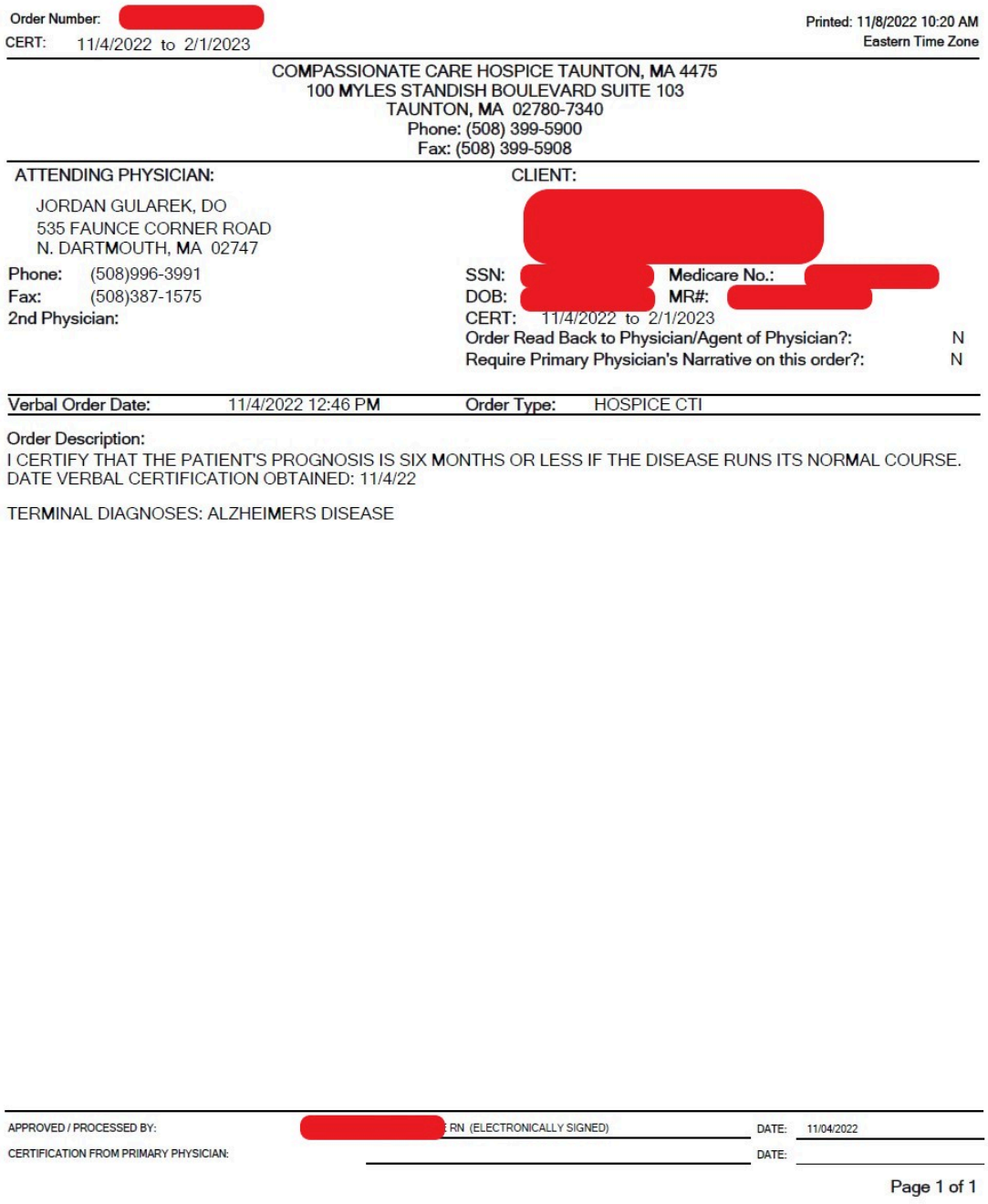
Psychosocial: [redacted]

Additional Information: --

DME & Supplies
Gauze Pads. Exam Gloves. Chux/Underpads. , n/a, Colostomy supplies

Home health certification and plan of care for a female patient in New Mexico; Page 1 of the record for the patient, who has Stage 4 rectal cancer. Image redacted by DataBreaches.net.

The second screenshot, below, certifies that a Massachusetts patient has a terminal diagnosis of Alzheimer's Disease and likely has six months or less to live. Such certification is required to make the patient eligible for hospice care.



Order Number: [redacted]
CERT: 11/4/2022 to 2/1/2023

Printed: 11/8/2022 10:20 AM
Eastern Time Zone

COMPASSIONATE CARE HOSPICE TAUNTON, MA 4475
100 MYLES STANDISH BOULEVARD SUITE 103
TAUNTON, MA 02780-7340
Phone: (508) 399-5900
Fax: (508) 399-5908

ATTENDING PHYSICIAN:
JORDAN GULAREK, DO
535 FAUNCE CORNER ROAD
N. DARTMOUTH, MA 02747
Phone: (508)996-3991
Fax: (508)387-1575
2nd Physician:

CLIENT:
[redacted]
SSN: [redacted] Medicare No.: [redacted]
DOB: [redacted] MR#: [redacted]
CERT: 11/4/2022 to 2/1/2023
Order Read Back to Physician/Agent of Physician?: N
Require Primary Physician's Narrative on this order?: N

Verbal Order Date: 11/4/2022 12:46 PM Order Type: HOSPICE CTI

Order Description:
I CERTIFY THAT THE PATIENT'S PROGNOSIS IS SIX MONTHS OR LESS IF THE DISEASE RUNS ITS NORMAL COURSE.
DATE VERBAL CERTIFICATION OBTAINED: 11/4/22

TERMINAL DIAGNOSES: ALZHEIMERS DISEASE

APPROVED / PROCESSED BY: [redacted] RN (ELECTRONICALLY SIGNED) DATE: 11/04/2022
CERTIFICATION FROM PRIMARY PHYSICIAN: DATE:

Page 1 of 1

Certification that a patient doesn't have long to live so that they can get hospice care. Image: DataBreaches.net

Many of the reports in the data Kazu provided to this site were for home health care for occupational therapy, physical therapy, visiting nurse services, or hospice services. All of the files examined by DataBreaches contained personal and protected health information.

HIPAA Concerns

Doctor Alliance is a firm with a presence in both the U.S. and India. According to what Kazu claims, the majority of employees are in India, but if Doctor Alliance is doing business in the U.S. and providing services involving

electronic billing transactions, then they should have business associate agreements (BAA) in place with HIPAA-covered entities, and they need to comply with HIPAA and HITECH notification requirements.

DataBreaches does not know exactly how many HIPAA-covered entities Doctor Alliance has had over the past six years or so (considering the dates of some of the medical records), but they may have thousands of notifications to make to former or current clients, and if their BAA calls for it, they may have hundreds of thousands — or more — individual notifications to be sent to affected patients.

But apart from any regulatory notification requirements that they may be subject to and other incident response costs that may or may not be covered by any insurance, there is the issue of whether their network is secure enough at this point for clients to trust.

From what Kazu shared with DataBreaches, the CEO of Doctor Alliance appears to have been informed by Availity that the payment platform would "reenable the blocked users and connections associated with Company after you complete a full breach assessment of Company's affected systems ("Breach Assessment")." Availity's communication includes a very specific and detailed list of questions about the entity's security, incident response, and required attestation that the network is now clean. In light of the second attack *after* Doctor Alliance claimed the vulnerability was corrected the same day as the first attack, it appears that Doctor Alliance did not have a full understanding of their security issues. Could Kazu successfully compromise them again? One hopes not, but it would be understandable for Doctor Alliance's clients to be seriously concerned at this point.

DataBreaches emailed Doctor Alliance earlier today to ask for an update and response to the second breach, but has received no reply. DataBreaches also emailed Availity to ask if their alleged communication to the CEO represents a routine incident response for them, and if they are aware of the second claimed attack. No reply was immediately available.

As this post was about to be published, Kazu contacted this site to say he was about to leak all the data, so there may be another update soon.

Update 1: Over on *SuspectFile*, Marco A. De Felice discusses these breaches and how Doctor Alliance's lack of transparency makes it impossible for their clients to really trust that their data has not been stolen or won't be stolen by Kazu again. Doctor Alliance clearly tried to reassure its clients after the first attack, but given that they were proven wrong in their claims, can any client believe that their data hasn't been acquired?

As a matter of common sense, you can't assure clients that their data is safe or wasn't acquired if you haven't finished a complete forensic investigation, and it doesn't sound like they have. So how can they reassure any client(s) that their data has not been compromised or is not at risk of further compromise? Once covered entities are aware of a breach, they have obligations under HIPAA, including not knowingly uploading PHI to an unsecured environment or possibly unsecured environment.

Read Marco's thoughtful commentary on SuspectFile.

Update 2 (November 20): Kazu has leaked the 1.2 TB of data.
