The Daily Swig
Cybersecurity news and views

Breach at Deep South allergy clinic group exposed the health info of estimated 9,800 patients

Emma Woollacott 26 August 2021 at 13:50 UTC
Updated: 26 August 2021 at 15:08 UTC

Data Leak | Healthcare | US

Data leak might be linked to ransomware gang's data dump

Atlanta Allergy & Asthma (AAA), the largest allergy treatment healthcare business in the region, is notifying 9,800 patients that a January data breach involved protected health information.

Miscreants extracted full names, birth dates, Social Security numbers, diagnoses, treatment information, and costs, along with provider names, financial account numbers, treatment location, dates of service, and patient health insurance information.

The breach took place between January 5 and January 13.

"Upon learning of the issue, AAA immediately took steps to secure its network and mitigate against any additional harm. AAA worked very closely with external cybersecurity professionals to determine the full impact of the incident," the firm said in a statement.

"To date, AAA is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident."

It recommends that those affected should consider credit monitoring services, or placing a fraud alert or security freeze on their credit files.

Early warning ignored?

However, while AAA says it first spotted the breach on July 8 and is only now notifying patients, it was first reported to the company back in March.

Anonymous healthcare privacy blog Databreaches.net spotted the data on the dark web, where it had been posted by the Nefilim ransomware group, also known as Nempty.

"The 1.3 GB compressed archive extracted to 2.5 GB of data consisting of 597 files with PHI [Protected Health Information] on what appears to be thousands of named patients," it reported.

"The files are not just current or recent billing-related files: spreadsheets organized by type of health insurance, including records on outstanding claims from 2017 and 2018 were also dumped in the 'Electronic Remits' folder, as were more than 100 audits, where each audit might be a multi-page detailed review of a patient's case."

Databreaches.net says it received no acknowledgement of its report from AAA, but that it notified the Department of Health and Human Services (HHS) on April 5.

"How can this possibly be acceptable? Spoiler alert: in my opinion, it's not," the author writes.

Latest Posts

Remote takeover
Microsoft warns of critical Azure CI vulnerability impacting Cosmos DE accounts

Video surveillance
Annke NVR flaw could see attacke control of security cameras

Singapore eye clinic potentia breaches 73,000 patients' da
Healthcare provider hit by cyber-at earlier this month

"If HHS wants the 'no later than 60 days' taken seriously, it really needs to take enforcement action in some cases."

The Daily Swig has invited AAA to respond. We will update the article should we receive a reply.

RELATED Whistleblowing security researchers deny 'inappropriate access' to Indiana Covid-19 survey data

Data Leak | Healthcare | US | Privacy | North America | Data Breach | Database Security | Ransomware | HIPAA | Network Security

Emma Woollacott

@EmmaWoollacott

Related stories

Remote takeover

Microsoft warns of critical Azure Cloud vulnerability impacting Cosmos DB accounts

27 August 2021

Video surveillance

Annke NVR flaw could see attackers seize control of security cameras

27 August 2021

Singapore eye clinic potentially breaches 73,000 patients' data

27 August 2021

Dating location leak

'Trilateration' vulnerability in Bun revealed users' exact position

26 August 2021