Norton Healthcare discloses data breach after May ransomware attack

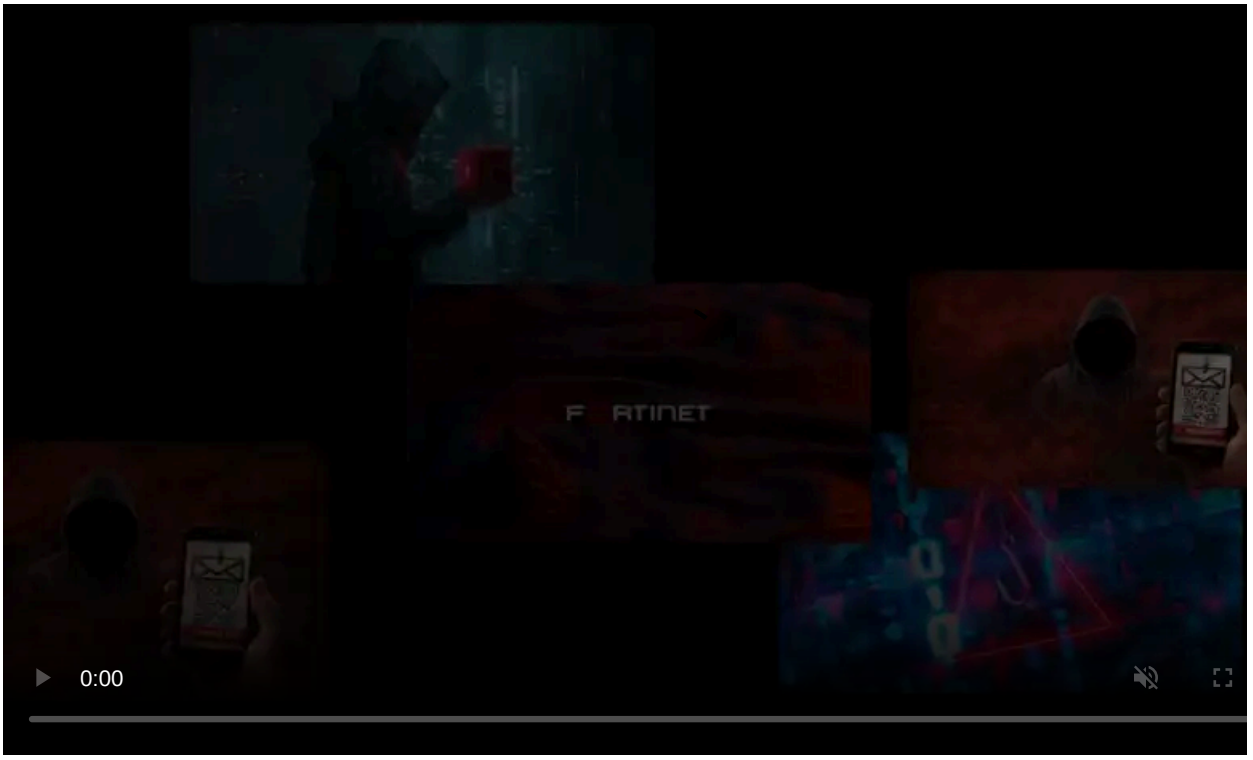
By Sergiu Gatlan

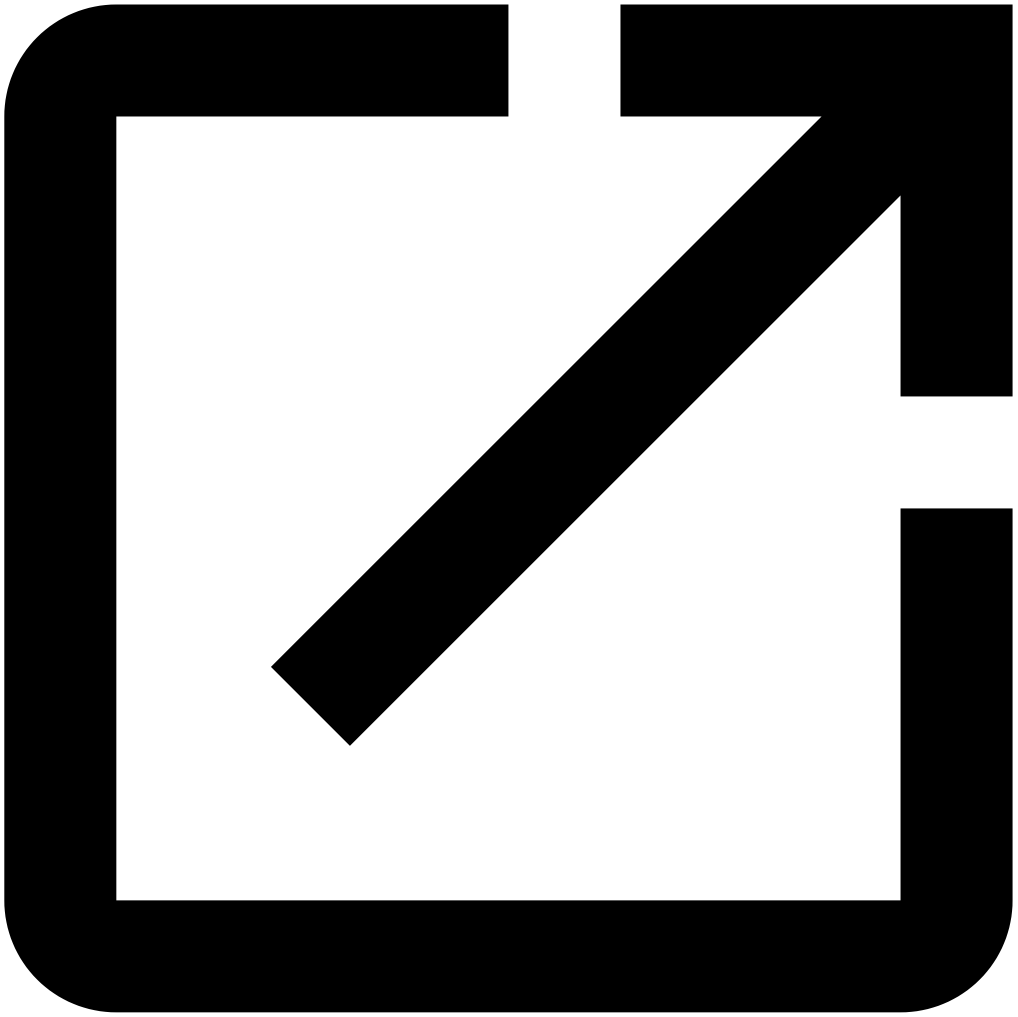
Published: 2023-12-08 · Archived: 2026-04-06 00:17:24 UTC

Kentucky health system Norton Healthcare has confirmed that a ransomware attack in May exposed personal information belonging to patients, employees, and dependents.

Norton Healthcare serves adult and pediatric patients in more than 40 clinics and hospitals across Greater Louisville, Southern Indiana, and the Commonwealth of Kentucky.

With over 20,000 employees, more than 1,750 employed medical providers, and over 3,000 total providers on its medical staff, Norton Healthcare is Louisville's second-largest employer, with more than 140 locations throughout Greater Louisville and Southern Indiana.


F RTINET
0:00



Roughly 2.5 million individuals had their data exposed in the attack, according to breach notification letters sent to those affected by the data breach.

"On May 9, 2023, Norton Healthcare discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack," it said in a press release published on Friday.

"Norton Healthcare notified federal law enforcement and immediately began working with a respected forensic security provider to investigate and terminate the unauthorized access.

"Our investigation determined that an unauthorized individual(s) gained access to certain network storage devices between May 7, 2023, and May 9, 2023, but did not access Norton Healthcare's medical record system or Norton MyChart."

The attackers gained access to a wide range of sensitive information, including name, contact information, Social Security Number, date of birth, health information, insurance information, and medical identification numbers.

Norton Healthcare says that, for some individuals (likely employees), the exposed data may have also included financial account numbers, driver's licenses or other government ID numbers, and digital signatures.

Potentially affected individuals will receive two years of free credit protection services and additional information in breach notification letters.

Ransomware attack claimed by BlackCat/ALPHV

While Norton Healthcare didn't link the attack to a specific ransomware operation, the attack was claimed in late May by the ALPHV (BlackCat) gang.

The attackers claimed in an entry added to their dark web leak site that they allegedly stole 4.7TB of data from the healthcare system's compromised systems, as DataBreaches reported.

The ransomware gang also leaked dozens of files as proof of the breach and data exfiltration, containing some Norton Healthcare patients' Social Security numbers, bank statements, and more.

BleepingComputer reported today that an ongoing outage affecting ALPHV's websites could be connected to a law enforcement operation.

Norton Healthcare is just one of a long string of healthcare organizations in the United States that have fallen victim to ransomware.

For instance, healthcare provider Ardent Health Services, which operates 30 hospitals across six U.S. states, also disclosed last month that it was hit by a ransomware attack.

Since last year, the U.S. government has issued multiple cautionary advisories regarding ransomware attacks targeting healthcare institutions nationwide.

One such advisory came from the security team at the U.S. Department of Health and Human Services (HHS) about ransomware operations like Royal, Venus, Maui, and Zeppelin targeting Healthcare and Public Health (HPH) organizations.

In October 2022, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the HHS notified hospitals about the Daixin Team cybercrime gang's active targeting of healthcare facilities in ransomware attacks.

Update: Added info on the number of affected individuals.

Source: https://www.bleepingcomputer.com/news/security/norton-healthcare-discloses-data-breach-after-may-ransomware-attack/