# A criminal actor is to blame for a dayslong cyberattack on a Chicago hospital, officials say

February 8 2024, by Kathleen Foody


Lurie Children's Hospital sign is seen at the hospital as patients walk in, Monday, Feb. 5, 2024, in Skokie, Ill. A Chicago children's hospital has been forced to take its networks offline after an unspecified digital attack, limiting access to medical records and hampering communication by phone or email since the middle of last week. Credit: AP Photo/Nam Y. Huh

A large children's hospital in Chicago remains hobbled by a cyberattack that began more than a week ago, cutting doctors and nurses off from digital patient records and limiting parents' ability to communicate with their kids' caregivers.

Officials at Lurie Children's Hospital said Thursday that they are still working with the FBI and other law enforcement but told reporters that a "known criminal threat actor" had accessed the hospital's network.

The hospital shut down its own systems for phone, email and medical records once the breach was discovered on Jan. 31, officials said.

"We take this matter very seriously and have been working closely around the clock with outside and internal experts and in collaboration with law enforcement, including the FBI," said Dr. Marcelo Malakooti, Lurie's chief medical officer. "This is an active and ongoing investigation."

The situation at Lurie Children's Hospital had all the hallmarks of a ransomware attack, although hospital officials have not confirmed or denied the cause. Such extortion-style attacks are popular among ransomware gangs seeking financial gain by locking data, records or other critical information, and then demanding money to release it back to the owner.

Allan Liska, an analyst with cybersecurity firm Recorded Future, said victims often are advised not to name specific criminal groups but said the description Lurie officials provided Thursday suggests it's an operation well known to U.S. law enforcement.

"Even though we all know most hospitals with some exceptions don't have spare cash to pay a large ransom, they're much more aggressive than they used to be when going after health care providers," Liska said

of ransomware gangs' strategies.

Lurie Children's Hospital logo is seen at the hospital, Monday, Feb. 5, 2024, in Skokie, Ill. A Chicago children's hospital has been forced to take its networks offline after an unspecified digital attack, limiting access to medical records and hampering communication by phone or email since the middle of last week. Credit: AP Photo/Nam Y. Huh

A representative for the FBI in Chicago would not provide further information on the hospital's comments, referring The Associated Press to a statement released Wednesday confirming an ongoing investigation.

The U.S. Department of Health and Human Services warned in a report

last year that health care providers have increasingly been targeted by criminals, causing delayed or disrupted care for patients across the country.

But schools, courts, utilities and government agencies all have been exposed.

Lurie has directed patients to use a call center and said it can help people refill prescriptions, discuss appointments and reach health care providers.

"We recognize the frustration and concern the situation creates for all of those impacted," Malakooti said Thursday. "We are so grateful for this community for the outpouring of support, and we are especially inspired by our workforce and their resilience in their commitment to our mission."

But some parents have reported the center isn't keeping up with their needs, leaving families uncertain when they can get answers.

Brett Callow, a threat analyst with cybersecurity firm Emsisoft, said it can take weeks for a hospital to restore normal operations after a cyberattack, prioritizing critical systems first.

The latest annual report for Lurie Children's said staff treated around 260,000 patients last year. Chicago-area pediatrician practices that work with the hospital also have reported being unable to access digital medical records because of the attack.



Citation: A criminal actor is to blame for a dayslong cyberattack on a Chicago hospital, officials

say (2024, February 8) retrieved 16 August 2024 from https://techxplore.com/news/2024-02-criminal-actor-blame-dayslong-cyberattack.html