TechXplore

Cyberattack on top Indian hospital highlights security risk

December 7 2022, by Aniruddha Ghosal

ilbs
Department of Health & Family Welfare, GNCTD
25TH HEPATITIS DAY
DECEMBER 3, 2022
"Hepatitis Elimination: A social responsibility"
Institute of Liver and Biliary Sciences, GNCTD, D-1, Vasant Kunj, New Delhi-110070, Tel. + 91 11 46300000, Web: www.ilbs.in
पैदल यात्री

Patients and their attendants squat outside the All India Institute of Medical Sciences (AIIMS) hospital in New Delhi, India, Wednesday, Dec. 7, 2022. The leading medical institute in India's capital limped back to normality on Wednesday after a cyberattack crippled its operations for nearly two weeks. Credit: AP Photo/Altaf Qadri

The leading hospital in India's capital limped back to normalcy on Wednesday after a cyberattack crippled its operations for nearly two weeks.

Online registration of patients resumed Tuesday after the hospital was able to access its server and recover lost data. The hospital worked with federal authorities to restore the system and strengthen its defenses.

It's unclear who conducted the Nov. 23 attack on the All India Institute of Medical Sciences or where it originated. Hospital authorities didn't respond to requests for comment.

The attack was followed by a series of failed attempts to hack India's top medical research organization, the Indian Council of Medical Research. This raised further concerns about the vulnerability of India's health system to attacks at a time when the government is pushing hospitals to digitize their records.

More than 173,000 hospitals have registered with a federal program to digitize health records since its launch in September 2021. The program assigns patients numbers that are linked to medical information stored by hospitals on their own servers or in cloud-based storage. Experts fear that hospitals may not have the expertise to ensure digital security.

"Digitizing an entire health care system without really safeguarding it can pretty much kill an entire hospital. It suddenly stops functioning," said Srinivas Kodali, a researcher with the Free Software Movement of India.

That is what happened to the hospital in New Delhi. Healthcare workers couldn't access patient reports because the servers that store laboratory data and patient records had been hacked and corrupted.

The hospital normally treats thousands of people a day, many of whom travel from distant places to access affordable care. Always crowded, queues at the hospital grew even longer and more chaotic.

"The entire system isn't working because of the hack," said Deep Ranjan, who came to New Delhi from northeastern Assam state. He said he had spent five days waiting in line and still has not seen a doctor.

Sandeep Kumar, who accompanied his ill father, said the digital attack meant that appointments couldn't be booked online, and that doctors could do little when they saw patients because they couldn't access their medical history.

"We are digitizing (everything), but then there is an attack on the country's most important medical institute," he said.

On Nov. 30, there were repeated but ultimately unsuccessful attempts to breach the website of the Indian Council of Medical Research, the Press Trust of India news agency reported.

The attack on the hospital raised "serious questions about the cybersecurity of the country," said K.C. Venugopal, a member of Parliament from the main opposition Congress party.

India drafted a proposed law governing data privacy last month, but critics say it offers few safeguards to people. It has not yet been passed by Parliament.

Citation: Cyberattack on top Indian hospital highlights security risk (2022, December 7) retrieved 10 April 2024 from https://techxplore.com/news/2022-12-cyberattack-indian-hospital-highlights.html