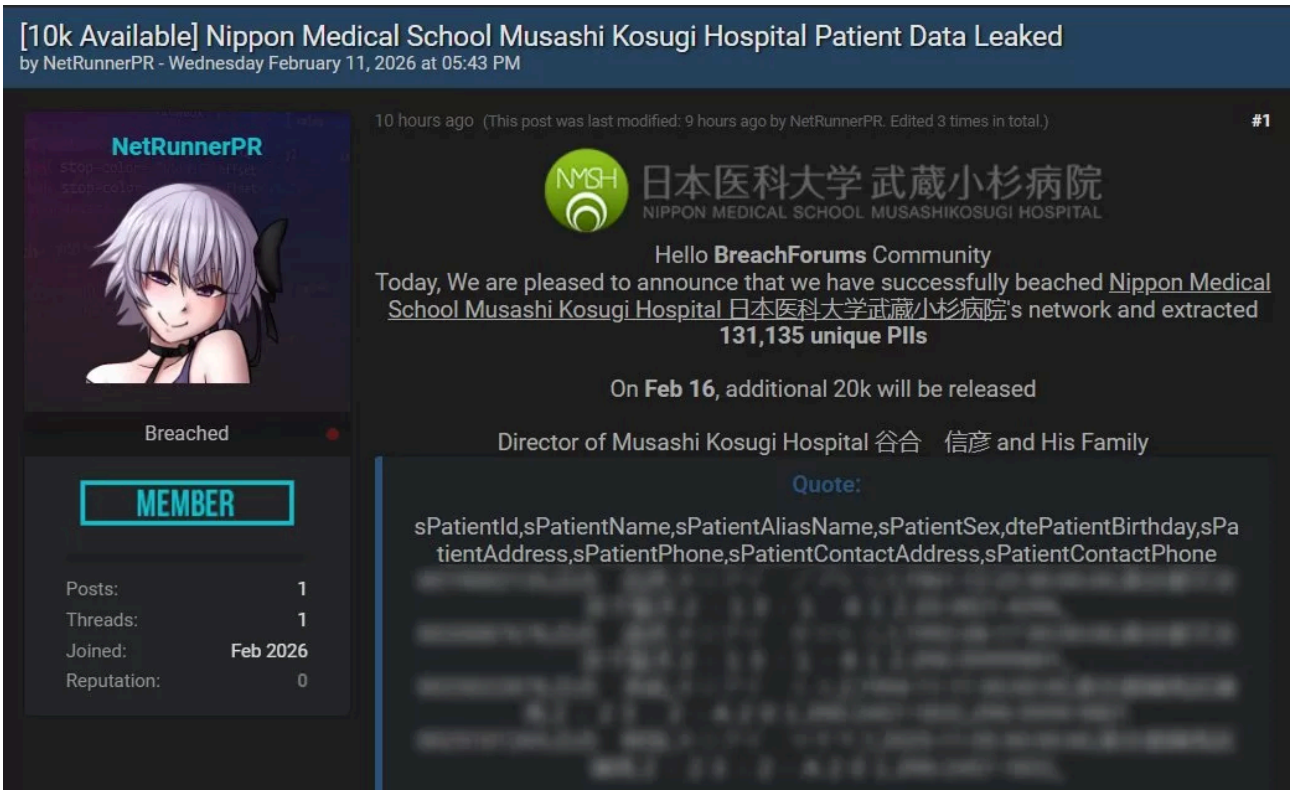
Nippon Medical School Musashi Kosugi Hospital Data Breach Claimed by NetRunnerPR

By Written by

Published: 2026-02-12 · Archived: 2026-04-02 11:50:45 UTC

A threat actor operating under the name “NetRunnerPR” has claimed responsibility for a cyberattack against Nippon Medical School Musashi Kosugi Hospital in Japan, alleging the exfiltration of 131,135 patient records. The claim was posted on a cybercrime forum on February 11, 2026, and includes what appears to be sample data intended to validate the breach.

Hospitals & Treatment Centers



At the time of writing, the alleged **Nippon Medical School Musashi Kosugi Hospital data breach** remains unverified. No official confirmation has been issued by the hospital, regulators, or Japanese authorities.

Breach Notification Service

What the Threat Actor Claims

According to the forum post, NetRunnerPR states that the hospital’s network was successfully breached and that 131,135 unique patient PII records were extracted. The actor further claims that an additional 20,000 records will

be released publicly on February 16, 2026, if certain undisclosed conditions are not met.

The dataset is described as containing personally identifiable information including:

- Patient ID numbers
- Full names and alias names
- Sex and date of birth
- Residential addresses
- Phone numbers
- Emergency contact details

The actor also referenced a hospital director and family members in the post, a tactic sometimes used in extortion campaigns to increase pressure on victims.

Analysis of the Sample Data

The forum listing includes what appears to be a partial CSV-style export. The visible header fields suggest structured database extraction rather than unorganized document theft. The column naming conventions indicate standardized internal record formatting.

However, the presence of sample data alone does not confirm the scope, authenticity, or recency of the dataset. Without independent forensic validation, it remains unclear whether:

- The records are recent or historical
- The dataset is complete or partial
- The information originates from internal systems or third-party providers
- The data has been altered or combined from previous breaches

Who Is NetRunnerPR?

NetRunnerPR appears to be a relatively new account on the forum where the claim was posted. As of the time of publication, the account shows limited activity history and minimal reputation metrics.

There is no publicly documented history tying NetRunnerPR to major ransomware operations or previously confirmed breaches. This lack of established track record introduces uncertainty regarding the credibility of the claim.

Threat actors frequently use newly created accounts to post high-profile breach claims, particularly in healthcare and education sectors, where sensitive data increases leverage.

Why Healthcare Breaches Are High Impact

Healthcare institutions are consistently among the most targeted sectors in cybercrime campaigns. Patient data is considered highly valuable because it often includes comprehensive identity profiles that can be used for fraud, identity theft, insurance abuse, and social engineering attacks.

Medical records typically contain stable identifiers such as full legal names, dates of birth, government-issued IDs, and long-term contact information. Unlike passwords, this type of data cannot easily be changed once exposed.

In Japan, healthcare organizations are subject to strict privacy and data protection requirements. If confirmed, the incident could trigger regulatory scrutiny and mandatory disclosure obligations under Japanese data protection frameworks.

Possible Attack Scenarios

At this stage, the intrusion vector remains unknown. Common entry points for hospital network compromises include:

- Phishing campaigns targeting staff
- Compromised remote desktop services
- Unpatched vulnerabilities in web-facing systems
- Third-party vendor access abuse
- Ransomware affiliate activity

The forum post does not explicitly mention ransomware encryption, suggesting the possibility of a data exfiltration-only operation. However, without official confirmation, the exact method of compromise remains speculative.

The Threat of Staggered Releases

The actor’s statement that 20,000 additional records will be released on February 16 follows a pattern commonly seen in extortion campaigns. Staggered release threats are designed to increase urgency and pressure organizations into negotiations.

Antivirus & Malware

Such tactics are frequently used in double extortion schemes, where attackers both encrypt systems and threaten public data exposure. However, no evidence currently confirms that encryption occurred in this case.

What We Do Not Yet Know

Several key questions remain unanswered:

- Has Nippon Medical School Musashi Kosugi Hospital confirmed a breach?
- Have Japanese regulators been notified?
- Is the dataset authentic and complete?
- Was ransomware deployed, or was this purely data theft?

- Are the affected individuals aware of potential exposure?

Until independent verification or official disclosure occurs, the claim should be treated as an alleged breach rather than a confirmed incident.

Current Status

As of February 11, 2026, the breach claim remains pending verification. No official public statements have been released by the hospital.

Data Backup Solutions

Botcrawl will continue monitoring developments related to the alleged Nippon Medical School Musashi Kosugi Hospital data breach and will update this article as additional verified information becomes available.
