UNM Health reports ransomware attack disrupting patient care and surgeries



A ransomware attack on UNM Health has reportedly disrupted patient care and surgeries. Only the headline of the report was available, so details are limited; healthcare providers should review their own ransomware readiness.

- UNM Health was hit by a ransomware attack, according to BleepingComputer.
- The reported impact includes disruption to patient care and surgeries.
- The source text available to us was unreadable beyond the headline, so no further details are confirmed.
- Healthcare operations depend on continuous system availability, which makes ransomware a patient-safety issue.

What was reported

BleepingComputer reports that a ransomware attack on UNM Health has disrupted patient care and surgeries. This is the only information we can confirm: the body of the article was not readable in the material we received, so we do not cite the attackers, the date, the systems affected, the scale of the disruption or the state of recovery.

Why it matters for the Kingdom

Hospitals and clinics rely on electronic records, scheduling, imaging and medical devices. When these systems become unavailable, clinical work slows or stops, and the effect reaches patients directly. Healthcare institutions in Saudi Arabia face the same type of risk, and they also hold sensitive personal health data that carries obligations under the PDPL.

Practical next steps

This incident is a useful prompt to test readiness rather than a reason for alarm. Leaders should confirm that the controls they already depend on would work under a real ransomware event, especially the ability to keep treating patients while core systems are offline. We will update this item if a fuller account becomes available.

What to do now

1. Test that clinical downtime procedures (paper records, manual scheduling, alternative routing of procedures) work for critical departments.
2. Verify that offline, immutable backups of key clinical systems exist and that a restore has been tested recently.
3. Review network segmentation between administrative IT, clinical systems and medical devices.
4. Confirm the incident response plan covers ransomware, including decision rights, communication with regulators and the NCA, and PDPL breach assessment.
5. Check that privileged accounts use multi-factor authentication and that remote access is tightly controlled.