Quest Diagnostics confirms patient records exposed in Quanum LSM breach



Quest Diagnostics says a threat actor gained unauthorized access to its Quanum LSM system, exposing patient records. The source excerpt gives no further detail on scope or timing.

- Quest Diagnostics, a US clinical laboratory company, has confirmed a data breach.
- A threat actor gained unauthorized access to the Quanum LSM system.
- Patient records were exposed as a result.
- The available source text does not state the number of people affected, the data types or the timeline.

What was reported

Quest Diagnostics, an American clinical laboratory company, has disclosed that patient records were exposed after an attacker obtained unauthorized access to its Quanum LSM system.

The text available to us is only an excerpt. It does not say how many patients are affected, which categories of data were involved, when the intrusion happened, or how the attacker got in. We have therefore left those points out and will not speculate on them.

Why it matters for regulated institutions

Laboratories and healthcare providers hold sensitive personal and health information, and they often depend on specialised platforms operated by the provider or by third parties. An incident in one such system shows how exposure of patient records can follow from a single point of unauthorized access.

Institutions in the Kingdom that handle health data, or that rely on laboratory and clinical platforms, may wish to use this disclosure as a prompt to review their own arrangements rather than wait for further detail.

Suggested next steps

Treat this as a reminder to confirm that access to systems holding patient data is tightly controlled and monitored, that third-party platforms are covered by your risk register, and that your breach notification process under the PDPL is ready to be used. Follow Quest Diagnostics' own communications for confirmed details as they are published.

What to do now

1. Review who and what can access systems holding patient or laboratory data, and remove unused or excessive access.
2. Confirm that logging and alerting cover unauthorized access to clinical and laboratory platforms.
3. Check that third-party health platforms appear in your risk register and that contracts require prompt incident notification.
4. Test your personal data breach response and notification process under the PDPL.
5. Monitor Quest Diagnostics' official updates and reassess exposure if you use related services.