Incident update (facts)

Stage 4 evidence

Open only after your initial two-plus-one recommendation (Stage 3) is complete.

To: Fatima Al-Sayed, GRC lead **From:** Aisha Rahman, IT, with Security operations **Date:** 2027-02-12 **Audience:** GRC and security leadership. Not a press statement.

What happened

Credential-stuffing traffic was observed against the **patient portal**. A large number of member-facing accounts experienced **account lockouts**.

Security operations required approximately **14 hours** to detect the pattern and complete initial scoping. Analysts had to pull and correlate events from **fragmented logs**.

What is not confirmed

There is **no confirmed member-record exfiltration**.

This update does **not** state that an unpatched portal vulnerability caused the incident.

Capacity

Response, customer support load, and portal hardening consumed approximately **three weeks** of the remediation capacity that steering was going to allocate to the two fully funded initiatives.

Constraints that did not move

The **August 2027 readiness milestone does not move**.

Steering wants a **residual-risk position within 10 days** (what we are funding, treating as interim, deferring, and accepting after this event).

What this note does not decide

This note does not name which two initiatives to fund. It does not state that any specific program must now be funded. Those choices remain a GRC recommendation to steering.