Operational history (clinic-ops and portal)

Compiled by Aisha Rahman (IT) for GRC, 2027-01-29. These are past operating facts. They are not a current incident packet.

Detection lag (2026)

A suspicious authentication burst against an internal admin tool was noticed late because analysts had to pull **three log stores** and reconcile timestamps. Scoping took most of a business day after the first alert. No member records were confirmed stolen in that event. The post-incident note said fragmented logging slowed the timeline. It did not fund a logging program.

Restore (2026)

A clinic-ops restore test was scheduled and then **stopped before completion** because the test collided with a clinic go-live rehearsal. Engineering still does not have a completed restore that meets the 4-hour policy RTO. First engineering judgment, if asked today: an evidenced restore would more likely land near **72 hours**, not 4 hours, unless the program is actually funded and tested.

Clinic-West

Operations still routes a non-trivial share of appointments through a path that **appears** to touch Clinic-West components (see inventory caveat). A 2026 sunset memo said Clinic-West was "planned for decommission." No decommission date was met.

Change tickets

Spot checks of last quarter's production releases found tickets with missing test notes and missing back-out steps. Some releases had complete tickets. The process is not absent. The evidence is unreliable.