Engineering estimates (clinic-ops and portal)

From: Jordan Ellis, Engineering **To:** GRC / Security **As of:** 2027-01-30 **Confidence:** stated per row. Point estimates are not commitments.

Clinic-ops has a **product freeze** targeting **2027-06-15** because of a contractual clinic go-live. Disruptive production testing after that date needs a freeze exception from Luis Navarro (CTO) and Mei Lin (VP Clinic Operations).

Calendar reality: from freeze date 2027-02-02 to the readiness week of 2027-08-03 is about **26 calendar weeks**. Engineering does not have 26 weeks of dedicated remediation capacity. Two full workstreams is the planning assumption. A third full program does not fit.

Point estimates

ID	Work if fully funded	Point estimate	Last similar effort (actual)	Confidence	Disruption
R1	Centralized logging for confirmed clinic-ops production and portal, plus alerting on high-value sources	**8 weeks**	Last telemetry centralization: **16 weeks**	Low to Moderate	Low to Moderate (agent rollout, log volume)
R2	Evidenced restore of clinic-ops to the policy RTO, including a production-like restore test	**6 weeks**	Last DR drill attempt: **9 weeks** and the restore was **not completed**	Moderate	**High** during the restore test (needs freeze-window exception if it lands near June)
R3	Broad portal hardening (production findings plus systematic dependency refresh and header policy)	**10 weeks**	Last portal hardening: **12 weeks**	Moderate	Low to Moderate
R4	Full Clinic-West remediation (inventory, rebuild or replace, remove standing local admin, cut leftover production path)	**14 weeks**	Last site-stack migration: **18 weeks**	Low	Moderate to High if replacement proceeds
R5	Full change-management program refresh (tooling, CAB redesign, training)	**8 weeks**	Last ITSM evidence project: **11 weeks**	Moderate	Low if limited; higher if a new CAB is forced onto product teams during freeze

Scoped work Engineering can describe (not a recommended portfolio)

These are **capacity facts**, not GRC's answer. They exist so you can design treatments of different sizes.

Logging (R1). Engineering can start centralized collection on **already confirmed** clinic-ops production and portal systems without waiting for a Clinic-West replacement program. Coverage **cannot** be claimed for unidentified Clinic-West hosts. Retention can be increased on some existing stores in days, not weeks. Temporary manual review and escalation can be staffed while remaining sources are scheduled after August. A highest-value-systems-first design is smaller than full coverage.

Portal backlog (R3). Confirmed **production High** items are a smaller slice than the 10-week hardening program. Scan and review cadence can be increased without the full program. Deferred findings can be exception-listed with owners. Staging findings are not production work.

Clinic-West (R4). Confirming whether Clinic-West is in the production path, naming an owner, freezing standing local admin use, and network-restricting the leftover hosts is **not** a 14-week replacement. Full rebuild remains a program.

Change evidence (R5). An evidence pack for production changes on **high-value systems** is smaller than a CAB redesign. Engineering can pull tickets for a defined population on a defined window.

DR (R2). A tabletop is not an evidenced restore. A single-system restore demonstration is smaller than a full RTO program, but it still needs a test window.

Dependency note (logging and Clinic-West)

Centralized logging **depends to some degree** on knowing which systems are production. Clinic-West inventory is incomplete, so logging coverage for those hosts cannot be honest until they are identified and owned.

That is **not** the same statement as "R1 cannot start until R4 is fully remediated." Logging on confirmed clinic-ops and portal systems can proceed. A scoped Clinic-West inventory/ownership effort can enable broader logging claims later. A full Clinic-West replacement is a different, larger job.

If a dependency slips (for example, inventory confirmation slips), coverage claims and alerting scope slip with it. Sequence the work so a slip has a named consequence, not a silent gap.

Cost figure circulating in planning slides

Someone put **$184,200** on an R1 slide. Engineering did not produce that number. Treat it as **low-confidence decoration** unless Finance confirms it. Do not let a precise figure substitute for the capacity constraint (two full workstreams).