Security risk summary (five issues)

Author: Harborline Security (compiled for GRC, 2027-01-28) **Scope:** clinic-ops production platform and patient portal only **Ratings:** Security's current labels. These are inputs, not a required funding order.

Harborline asked Security for a short list. There are **five** issues. Do not add a sixth initiative to this cycle.

R1. Centralized security logging (clinic-ops production and patient portal)

Security rating: High

Production authentication, administrative, and key application logs for clinic-ops and the patient portal sit in **separate stores** with uneven retention. Security operations can retrieve events, but correlation across systems is slow and incomplete. Coverage claims cannot currently be made for every host that might be in the production path.

Security's preferred end state is a centralized store with defined retention and alerting for high-value systems. That is a program, not a weekend change.

R2. Disaster-recovery restore assurance (clinic-ops)

Security rating: High

Policy states a **4-hour RTO** for clinic-ops production. Security has **no evidenced restore** that met that objective. Backups are taken. Restore *assurance* is the gap.

A failed or slow restore would stop clinic scheduling and related operations. This is an availability and customer-commitment issue, not only a policy paperwork issue.

R3. Patient-portal vulnerability backlog

Security rating: High

The portal scanner and the last targeted review produced a mixed backlog:

Finding	Environment	Severity (scanner)	Notes
Session handling weakness	Production	High	Confirmed by Engineering as production
Outdated dependency in auth library	Production	Medium	Patch available; change window required
Verbose error content	Production	Low	Cosmetic unless combined with other issues
Privileged debug interface exposed	**Staging**	**High**	Staging is not production. Not reachable from the public portal URL.
Content-security-policy missing on marketing pages	Production	Medium	Marketing host is not the authenticated portal

Treat scanner severity as a claim. Confirm environment before you treat a row as a production emergency.

R4. Legacy Clinic-West uncertainty

Security rating: Medium-High

Clinic-West is a leftover clinic site stack. CMDB completeness is poor. At least some hosts have **standing local administrator** accounts. Whether Clinic-West still sits in the **production scheduling path** is not a closed question (see inventory caveat).

Security cannot currently attest that Clinic-West is out of production, fully inventoried, or free of standing privileged local access.

R5. Change-management evidence for production releases

Security rating: Medium

Production releases occur. Ticket quality is uneven. For some changes, Security cannot show who approved what, what was tested, or how the change was backed out. This is weaker than a missing change process. It is missing **evidence** that the process ran on the systems that matter.

Security did not rate this High. Readiness reviewers may still ask for it.

Out of this five-issue list

A company-wide phishing-awareness campaign is in the 2027 engagement backlog. It is not one of the five issues Security was asked to rank for this steering cycle.