RANSOMWARE READINESS CHECKLIST

Monthly quick-check for healthcare environments

Backup & Recovery

- Validate **offline/immutable** backups exist for **EHR, PACS, LIS, AD**, and critical infra; verify **last-success** times.
- Perform a **test restore** of representative data in an **isolated** environment; document **RTO/RPO**.
- Ensure backup networks/storage are **segmented** from production; **MFA** required for admin access.

Incident Contacts & Runbooks

- Update **on-call rosters** (IT, Clinical Leadership, Compliance/Privacy, Facilities, Comms); print copies.
- Confirm contracts/contacts for **IR retainer, cyber insurer, legal, EHR vendor, critical third parties**.
- Review **downtime procedures** (EHR read-only, manual charting, diversion plans); run a **15-minute tabletop**.

Endpoints, Identity & Network

- Verify **EDR** active/reporting on servers/workstations; spot-check alerts (use approved safe tests only).
- Patch **OS/apps**; track **medical-device exceptions** with compensating controls.
- Review **privileged accounts**; remove stale users; enforce **MFA** on remote access, VPN, admin consoles.
- Harden network: no **exposed RDP**, restrict **SMB**, segment **clinical VLANs**, add **egress filtering** from sensitive zones.

Email & SaaS

- Review **Microsoft 365/Google Workspace** security policies; enable **phishing/safe links/attachment** protections.
- Check **SPF/DKIM/DMARC** alignment and enforcement; auto-quarantine failures.

Awareness & Compliance

- Deliver **monthly micro-training** and a realistic **phishing simulation**; track completion by department.
- Confirm **breach-notification** and **OCR** reporting procedures are current; record legal sign-off.

Monthly Notes / Follow-ups