TheCyberOS

Total Control - Zero Compromise

Making you Powerful, Fearless, and Unstoppable against cyber attacks

Making you Powerful, Fearless, and Unstoppable against cyber attacks.

Audit Ready Checklist

1) Governance and Documentation (Administrative)

- ✓ **Security Official assigned** (name/role documented)
  - **Evidence:** org chart/policy header with owner
- ✓ **HIPAA Security Risk Analysis completed** within the last 12 months (and after major changes)
  - **Evidence:** risk analysis report + risk register
- ✓ **Risk Management Plan** with prioritized remediation, dates, and status
  - **Evidence:** remediation tracker/ticket export
- ✓ **Policies & Procedures** approved and current: access control, incident response, device/media, backups, vendor management
  - **Evidence:** policy packet with version history
- ✓ **BAAs on file** for all vendors touching ePHI (HER, imaging, billing, cloud, IT/MSP, backup, email, etc.)
  - **Evidence:** executed BAAs + vendor list

2) Workforce Safeguards (Administrative)

- ✓ **HIPAA security training completed annually** for the entire workforce (including temps)
  - **Evidence:** training roster + completion certificates
- ✓ **Phishing awareness** conducted at least quarterly (or equivalent)
  - **Evidence:** phishing test reports + corrective actions
- ✓ **Onboarding/Offboarding checklist** used every time (accounts created/disabled promptly
  - **Evidence:** completed checklist/HR ticket logs

3) Access Control and Identity (Technical)

- ✓ **Unique user IDs** for all systems; **no shared logins**
  - **Evidence:** user list export/access review
- ✓ **MFA is enabled** for email, remote access, EHR/admin portals, and privileged accounts
  - **Evidence:** MFA enforcement screenshot/policy
- ✓ **Least privilege** enforced; admin rights restricted and reviewed quarterly
  - **Evidence:** admin group membership + quarterly access review signoff
- ✓ **Password and lockout standards** enforced (or SSO)
  - **Evidence:** system policy settings

4) Device, Endpoint, and Network Controls (Technical)

- ✓ **Supported OS only:** patching in place (OS + apps)
  - **Evidence:** patch compliance report
- ✓ **EDR/AV installed** and monitored on all endpoints and servers
  - **Evidence:** endpoint coverage report + alert log sample
- ✓ **Disk encryption** enabled on laptops/workstations storing ePHI
  - **Evidence:** encryption status report
- ✓ **Firewall + secure remote access** (no exposed RDP/VPN or equivalent)
  - **Evidence:** network diagram + remote access configuration
- ✓ **Email protections** (SPF/DKIM/DMARC or equivalent)
  - **Evidence:** domain/email security settings

5) Backup, Recovery, and Downtime Readiness (Resilience)

- ✓ **3-2-1 backups,** including **off-site, immutable,** or otherwise ransomware-resistant copies
  - **Evidence:** backup architecture summary + immutable retention settings
- ✓ **Backups monitored daily** (success/fail alerts reviewed)
  - **Evidence:** monitoring dashboard/alert tickets
- ✓ **Restore tests performed** at least quarterly (include EHR-critical workflow)
  - **Evidence:** test logs with date, scope, results, and fixes
- ✓ **Written Contingency Plan:** data backup plan, disaster recovery plan, emergency mode operations plan
  - **Evidence:** signed plan + revision history
- ✓ **Downtime Procedures:** paper workflows, scheduling, prescriptions, lab orders, patient communications
  - **Evidence:** downtime binder + staff quick reference sheet

6) Incident Response and Breach Handling

- ✓ **Incident Response Plan** with roles, contacts, and decision tree
  - **Evidence:** plan + call tree (MSP, legal, insurer, forensics)
- ✓ **Breach notification workflow** defined (who decides, who notifies, timeliness)
  - **Evidence:** breach playbook + templates
- ✓ **Logging enabled** for key systems (EHR, email, firewall) and retained per policy
  - **Evidence:** logging configuration + sample log review

7) Physical and Facility Safeguards (Physical)

- ✓ **Server/Network gear secured** (locked room/cabinet; access limited)
  - **Evidence:** access list + photo/log
- ✓ **Workstation privacy** (screen locks, auto-timeout, clean desk)
  - **Evidence:** policy + spot-check record
- ✓ **Device/media disposal** documented (shred/secure wipe)
  - **Evidence:** disposal certificates/wipe logs

8) Quick Audit Packet (Have These Ready to Hand Over)

- Risk Analysis (latest) + remediation tracker
- Policies/procedures packet (versioned)
- Training roster + phishing results
- Vendor list + BAAs
- Backup/restore test logs + contingency plan
- Access review signoffs + MFA evidence
- Endpoint and patch compliance reports
- Incident response plan + last incident (even “none”)

Attestation: I confirm the above evidence exists and is current.

Security Official Signature: _____ Date:_____

A financial guarantee no one else dares to offer 48-hour SLA and up to one year of fees returned if your practice goes down.

Robert Owen – robert@currandata.com – 317-974-1008 ext. 1003