CORPORATE TECHNOLOGIES LLC
gocorptech.com

MEDICAL PRACTICE IT COST & RISK CONTROL CHECKLIST

Executive Decision Tool for Healthcare Practice Leaders

Built for medical practices (10–200 employees) responsible for patient data and operational continuity. Use this tool to evaluate IT cost alignment, downtime exposure, and security risk in under 30 minutes.

How to Use

1. Takes 20–30 minutes
2. Completed by IT Director, Network Admin, or CIO
3. Check each box that applies.
4. Count the total number of checked items.
5. Identify outage and security exposure

1 IT Spend & Financial Control

- ☐ Calculate annual IT spend as % of revenue
- ☐ Break down spend by category *support, security, hardware, software, cloud*
- ☐ List all recurring monthly IT contracts
- ☐ Define hardware replacement schedule (3–5 years)
- ☐ Estimate cost of 1 hour of downtime
- ☐ Ensure IT budget is planned yearly

2 Infrastructure & System Reliability

- ☐ Audit all servers, workstations, network devices
- ☐ Verify critical systems have vendor support
- ☐ Maintain current network diagram
- ☐ Test internet failover/redundancy
- ☐ Secure remote access via VPN
- ☐ Record system issues from last 12 months

3 Cybersecurity & Access Control

- ☐ Enable MFA for admin and remote accounts
- ☐ Install endpoint protection on all devices
- ☐ Audit access for terminated employees
- ☐ Conduct security training yearly
- ☐ Maintain incident response plan with contacts
- ☐ Monitor and update firewall regularly

4 Infrastructure & System Reliability

- ☐ Confirm daily automated backups: EHR and systems
- ☐ Store backups off-site or in secure cloud
- ☐ Test full data restoration in last 90 days
- ☐ Document RTO and RPO
- ☐ Keep disaster recovery plan written and accessible
- ☐ Assign responsibility for recovery plan

5

Compliance & Risk Management

- ☐ Complete HIPAA risk assessment yearly
- ☐ Maintain BAAs with IT vendors
- ☐ Enable encryption on laptops and mobiles
- ☐ Audit access logs for unusual activity
- ☐ Maintain written IT policies (passwords, remote work, device use)
- ☐ Document cybersecurity insurance coverage

Scoring Model

- Count the total number of checked items
- Total Possible Score: 30
- 0–10 → High Risk (Reactive and exposed)
- 11–20 → Moderate Risk (Operational but vulnerable)
- 21–30 → Controlled / Strategic (Proactively managed)

Immediate Red Flags

- Backups have not been restoration-tested in 90+ days
- No documented HIPAA risk assessment in last 12 months
- MFA not enforced for admin accounts
- IT spend percentage is unknown
- No documented disaster recovery plan exists
- No defined downtime cost per hour

Next Step

If your score indicates exposure or uncertainty, schedule a structured IT Risk & Cost Alignment Assessment.

Schedule a structured IT Risk & Cost Alignment Assessment