

Cybersecurity Readiness Checklist

Is your organization ready to face the cybersecurity challenges of today - and tomorrow?
Use this quick checklist to identify key gaps and ensure your systems, data, and people are protected.



Core Security Measures

- ☐ Multi-Factor Authentication (MFA) is enabled for all users
- ☐ Data encryption is in place for all patient records and backups
- ☐ Regular backups are scheduled, encrypted, and tested
- ☐ All critical systems and software are updated within 72 hours of patch release
- ☐ VPN is used for all remote access connections



Staff Awareness & Training

- ☐ Quarterly cybersecurity training is mandatory for all employees
- ☐ Phishing simulations are conducted and results are monitored
- ☐ Employees understand how to report suspected threats
- ☐ Role-based access controls are clearly defined and enforced



Strategic Oversight & Leadership

- ☐ Cybersecurity is discussed regularly at the leadership level
- ☐ A Chief Information Security Officer (CISO) or equivalent is assigned
- ☐ Annual risk assessments and penetration testing are conducted
- ☐ Vendor and third-party access is reviewed and monitored



Monitoring & Incident Response

- ☐ 24/7 system and network monitoring is in place
- ☐ An incident response plan is documented, tested, and reviewed
- ☐ Logs are collected and stored securely for audit purposes
- ☐ Breach notification policies are up to date and compliant



Final Step: Get Proactive

Cyber threats don't wait. Neither should your defense plan.

If you checked **fewer than 12 boxes**, now is the time to reassess your cybersecurity strategy.

Need help? Contact Healthcare ITSM for a free consultation: www.healthcareitsm.com

