Tower 23 IT HIPAA Compliance Checklist 2025

What Every Medical Practice Should Review This Year

Area	Key Tasks & Considerations
Risk Assessment (SRA)	☐ Conduct annual + event-triggered SRAs ☐ Use HHS/ONC SRA tools or NIST frameworks ☐ Document vulnerabilities and remediation plans
Compliance Officer	☐ Appoint Privacy & Security Officers (required by HIPAA) ☐ Define roles & responsibilities ☐ Ensure accountability and audit readiness
Policies & Documentation	☐ Maintain updated privacy/security policies, training logs, network maps, incident response plans ☐ Review annually and after system changes ☐ Test policies with mock audits or breach drills
Staff Training	☐ Train all staff at hire + annually (Privacy, Security, Breach Notification Rules) ☐ Simulate phishing attacks ☐ Add 2025 topics: AI, ransomware, telehealth tools ☐ Keep signed training logs
Technical Safeguards	☐ Encrypt PHI at rest and in transit ☐ Enable Multi-Factor Authentication (MFA) ☐ Use role-based access controls ☐ Apply automatic logoff/session timeouts ☐ Patch and update systems regularly

Business Associate Agreements (BAAs)	☐ Maintain signed Business Associate Agreements for all vendors handling PHI ☐ Include breach notification timelines (NPRM proposes 24 hours) ☐ Monitor vendor compliance and subcontractor use
Incident Response	☐ Maintain a written incident response and disaster recovery plan ☐ Define roles and responsibilities ☐ Conduct tabletop breach exercises annually ☐ Follow breach notification rules (60-day max)
Patient Access	☐ Provide patient records within 30 days (often faster) ☐ Support multiple formats (electronic, paper, portal) ☐ Comply with Information Blocking rules ☐ Charge only cost-based fees
Emerging Tech & Privacy	☐ Audit AI and machine learning use for PHI risks ☐ Review online tracking tools (cookies, analytics) ☐ Update Notices of Privacy Practices (NPPs) for reproductive health protections by Feb 2026
Audit Readiness	☐ Keep SRA documentation and remediation plans ☐ Maintain current training logs ☐ Document technical safeguards (encryption, MFA, access logs) ☐ Treat readiness as ongoing, not one-time prep