ORTHO-IT
Simplifying Technology So You Can
Focus on Smiles

Ortho-IT 2025 Edition

Security & Encryption

- [ ] PHI encrypted at rest and in transit (AES-256 or better)
- [ ] Full-disk encryption on all devices
- [ ] Secure VPN or TLS for remote access
- [ ] USB ports disabled or restricted
- [ ] Firewall and endpoint protection active and monitored

Access Controls

- [ ] Role-based access (least privilege principle)
- [ ] Unique user IDs and strong password policies
- [ ] Multi-factor authentication (MFA) for all PHI systems
- [ ] Automatic session timeouts and screen locks
- [ ] Access logs reviewed monthly

Backup & Disaster Recovery

- [ ] Daily encrypted backups of all PHI systems
- [ ] Offsite and cloud-based backup redundancy
- [ ] Documented restore procedures
- [ ] Annual disaster recovery drill completed
- [ ] Ransomware recovery plan in place

Risk Assessment & Audits

- [ ] Annual HIPAA risk analysis (NIST-based recommended)
- [ ] Vulnerability scans and penetration testing

- [ ] Audit logs enabled and retained for 6 years
- [ ] Incident response plan tested and documented
- [ ] Business Associate Agreements (BAAs) on file

Multi-Location Readiness

- [ ] Secure data syncing across locations
- [ ] Centralized access control and monitoring
- [ ] Consistent compliance policies across all offices
- [ ] Expansion checklist for onboarding new clinics
- [ ] Remote support and monitoring protocols

Patient Communication & Consent

- [ ] Secure email and messaging platforms
- [ ] Consent forms for electronic communication
- [ ] Patient portal with access controls and audit trail
- [ ] Breach notification procedures documented

Notes & Next Steps

HIPAA compliance isn't a checkbox—it's a culture. This checklist is your starting point. Let's build a system that protects your patients, your practice, and your peace of mind.

Need help implementing this?

Schedule a free consultation at ortho-it/contact