PHIPA Compliance Checklist

Use this checklist to evaluate your current security posture:

1. Access Control

- Unique user accounts for all staff
- Strong password policies enforced
- Multi-factor authentication enabled
- Access limited based on role
- Terminated employees removed immediately

2. System & Network Security

- Firewalls properly configured
- Endpoint protection installed and monitored
- Operating systems regularly updated
- Secure remote access (VPN or secure gateway)
- Wi-Fi separated for guests and internal systems

3. Data Protection

- Encrypted devices (laptops, workstations)
- Encrypted backups
- Secure cloud storage (if applicable)
- Email security and phishing protection
- Protection against ransomware

4. Backup & Recovery

- Regular automated backups

- Offsite or cloud backup copies
- Backup restore testing performed
- Documented recovery procedures

5. Policies & Documentation

- Written privacy and security policies
- Staff cybersecurity awareness training
- Incident response procedure documented
- Breach reporting process defined

Common PHIPA Risk Areas We See

Many healthcare providers believe they are compliant but discover gaps such as:

- Shared login accounts
- No MFA on email
- Backups never tested
- Unencrypted portable devices
- No documented incident response plan