

HIPAA Compliance Checklist for Business Associates

- We have a signed Business Associate Agreement (BAA) with all healthcare clients
- PHI is encrypted both at rest and in transit
- Multi-factor authentication (MFA) is enabled on all systems handling PHI
- Employee access to PHI is restricted based on job role (role-based access control)
- We provide regular HIPAA training for all staff
- We have documented policies and procedures for handling PHI
- A risk assessment has been completed within the last 12 months
- We have an incident response and breach notification plan in place
- All vendors with access to PHI are reviewed for compliance
- Our data backup systems are secure, tested, and HIPAA-compliant