CHECKLIST INTELLIGENT iT COMPLIANCE

HIPAA Compliance Quick-Start Checklist

Key safeguards every covered entity and business associate must implement.

HIPAA requires administrative, physical, and technical safeguards to protect electronic Protected Health Information (ePHI). Use this checklist to evaluate your compliance posture.

ADMINISTRATIVE SAFEGUARDS

- [ ] Designated HIPAA Privacy Officer and Security Officer appointed
- [ ] Comprehensive risk analysis conducted and documented (required annually)
- [ ] Risk management plan addresses identified vulnerabilities with remediation timelines
- [ ] Workforce training on HIPAA policies completed at hire and annually thereafter
- [ ] Business Associate Agreements (BAAs) executed with all vendors handling ePHI
- [ ] Sanctions policy documented for workforce members who violate HIPAA policies
- [ ] Contingency plan includes data backup, disaster recovery, and emergency operations

PHYSICAL SAFEGUARDS

- [ ] Facility access controls limit physical access to systems containing ePHI
- [ ] Workstation use policies define appropriate use and physical positioning of screens
- [ ] Workstation security: automatic screen lock, cable locks, and clean-desk policy enforced
- [ ] Device and media controls: inventory, disposal, and re-use procedures documented
- [ ] Visitor logs maintained for areas where ePHI is stored or accessible

TECHNICAL SAFEGUARDS

- [ ] Unique user identification: each user has a unique ID for ePHI system access
- [ ] Automatic logoff configured on all systems that access ePHI
- [ ] Encryption implemented for ePHI at rest and in transit (AES-256, TLS 1.2+)
- [ ] Audit controls: hardware, software, and procedures to record and examine access to ePHI
- [ ] Integrity controls ensure ePHI is not improperly altered or destroyed
- [ ] Access controls enforce minimum necessary standard — users access only required ePHI
- [ ] Multi-factor authentication required for remote access to systems containing ePHI

BREACH NOTIFICATION READINESS

- [ ] Breach notification procedures documented for individuals, HHS, and media (if 500+ affected)
- [ ] Incident response team trained on breach risk assessment (4-factor test)

- [ ] Breach log maintained for all incidents, including those determined not reportable
- [ ] Legal counsel identified for breach notification guidance