

HIPAA Audit Checklist

Use this checklist to assess whether your organization is HIPAA compliant and audit-ready before an OCR inquiry, customer review, or internal compliance assessment.

- ☐ A HIPAA Privacy Officer has been designated, and privacy policies are documented and maintained.
- ☐ All PHI locations and data flows have been identified across paper records, systems, email, and third-party vendors.
- ☐ Permissible uses and disclosures are documented, and disclosures requiring patient authorization are clearly defined.
- ☐ A current Notice of Privacy Practices is published, and patient rights request procedures are documented.
- ☐ An accounting of disclosures is maintained, and workforce privacy training is completed and documented.
- ☐ A HIPAA Security Officer has been designated.
- ☐ A current Security Risk Assessment has been completed, documented, and reviewed for gaps.
- ☐ Administrative safeguards are implemented, including workforce security, access management, security awareness training, and contingency planning.
- ☐ Physical safeguards are implemented, including facility access controls, workstation security, and device/media disposal procedures.
- ☐ Security incident response procedures are documented and ready to execute.
- ☐ Backup, disaster recovery, and emergency mode procedures are documented and current.
- ☐ Technical safeguards are in place, including unique user IDs, emergency access procedures, automatic logoff, and encryption for ePHI.
- ☐ Audit logs are enabled, reviewed regularly, and retained with required compliance documentation.
- ☐ Integrity, transmission security, and authentication controls are in place for ePHI systems and remote access.
- ☐ Breach risk assessment and notification procedures are documented, including workflows for 60-day notifications where required.
- ☐ Business Associate Agreements are executed before vendors access PHI, and vendor security reviews are performed and updated regularly.
- ☐ An audit-ready documentation set is assembled, including policies, risk assessments, training records, BAAs, incident records, and remediation evidence.
- ☐ An updated vendor inventory is maintained and reviewed annually.