HIPAA Audit Checklist

ORGANIZATION DETAILS

Name: _____ Address: _____

Contact Information: _____ HIPAA Compliance Officer: _____

I. PRIVACY RULE COMPLIANCE

Notice of Privacy Practices (NPP):

Notice of Privacy Practices Items

- [ ] Availability to patients
- [ ] Acknowledgment of receipt from patients
- [ ] Up-to-date content as per HIPAA requirements

Patient Rights:

Patient Rights Items

- [ ] Access to medical records
- [ ] Amendments to PHI (Protected Health Information)
- [ ] Accounting of disclosures
- [ ] Privacy complaints process

Use and Disclosure of PHI:

Use and Disclosure Items

- [ ] Minimum necessary standard applied
- [ ] Authorizations for use and disclosure
- [ ] Disclosures to family members and friends

Training and Awareness:

Training and Awareness Items

- [ ] Regular training for staff on HIPAA Privacy policies
- [ ] Documentation of training sessions

Safeguards:

Safeguards Items

- [ ] Administrative, technical, and physical safeguards
- [ ] Privacy policies and procedures documentation

II. SECURITY RULE COMPLIANCE

Risk Analysis and Management:

Risk Analysis and Management Items

- [ ] Regular risk assessments
- [ ] Implementation of security measures to reduce risks

Security Policies and Procedures:

Security Policies Items

- [ ] Written security policies and procedures
- [ ] Regular review and updates

Workforce Training and Management:

Workforce Training Items

- [ ] Security awareness training
- [ ] Sanction policies for violations

Information Access Management:

Information Access Items

- [ ] Access to PHI based on job role
- [ ] Procedures for granting access to PHI

Physical Safeguards:

Physical Safeguards Items

- [ ] Facility access controls
- [ ] Workstation and device security

Technical Safeguards:

Technical Safeguards Items

- [ ] Access control to electronic PHI (ePHI)
- [ ] Audit controls
- [ ] Integrity controls
- [ ] Transmission security

III. BREACH NOTIFICATION RULE COMPLIANCE

Breach Identification and Reporting:

Breach Identification Items

- [ ] Procedures for identifying breaches
- [ ] Timely reporting of breaches as per HIPAA guidelines

Documentation and Log Maintenance:

Documentation Items

- [ ] Documentation of identified breaches
- [ ] Log of breach notifications

IV. OMNIBUS RULE COMPLIANCE

Business Associate Agreements (BAAs):

Business Associate Agreements Items

- [ ] BAAs with all relevant vendors and third parties
- [ ] Regular review and updates of BAAs

Notice of Privacy Practices:

Notice of Privacy Practices Omnibus Items

- [ ] Inclusion of Omnibus Rule provisions

V. DOCUMENTATION AND RECORD KEEPING

Documentation and Record Keeping Items

- [ ] Policies and procedures documentation
- [ ] Training records
- [ ] Incident response and breach notification records
- [ ] Logs of access to PHI

VI. PERIODIC AUDITS AND ASSESSMENTS

Periodic Audits Items

- [ ] Regular internal audits
- [ ] External audits or assessments (if applicable)

VII. ACTION PLAN FOR NON-COMPLIANCE

Action Plan Items

- [ ] Identification of areas of non-compliance
- [ ] Action plan for addressing gaps
- [ ] Timeline for implementation

COMPLIANCE OFFICER'S SIGNATURE

Name: _____ **Date:** _____ dd / mm / yyyy

Disclaimer: This checklist is a tool for internal use and does not guarantee compliance. Regular consultation with legal experts in HIPAA regulations is recommended.