

HIPAA Audit Checklist

Organization Details:

Name: _____

Address: _____

Contact Information: _____

HIPAA Compliance Officer: _____

I. Privacy Rule Compliance

1. Notice of Privacy Practices (NPP):

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

2. Patient Rights:

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

3. Use and Disclosure of PHI:

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

4. Training and Awareness:

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

5. Safeguards:

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

II. Security Rule Compliance

1. Risk Analysis and Management:

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

2. Security Policies and Procedures:

- Written security policies and procedures
- Regular review and updates

3. Workforce Training and Management:

- Security awareness training
- Sanction policies for violations

4. Information Access Management:

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

5. Physical Safeguards:

- Facility access controls
- Workstation and device security

6. Technical Safeguards:

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

III. Breach Notification Rule Compliance

1. Breach Identification and Reporting:

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

2. Documentation and Log Maintenance:

- Documentation of identified breaches
- Log of breach notifications

IV. Omnibus Rule Compliance

1. Business Associate Agreements (BAAs):

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

2. Notice of Privacy Practices:

- Inclusion of Omnibus Rule provisions

V. Documentation and Record Keeping

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

VI. Periodic Audits and Assessments

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

VII. Action Plan for Non-Compliance

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

Compliance Officer's Signature

Name: _____

Date: _____

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