# HIPAA Compliance Checklist for Healthcare AI Projects

## Administrative Safeguards

### Security Management Process

- [ ] Conducted risk analysis to identify potential security vulnerabilities
- [ ] Implemented risk management procedures to mitigate identified risks
- [ ] Established sanction policy for workforce members who violate security policies
- [ ] Created information system activity review procedures

### Workforce Security

- [ ] Implemented procedures for authorization and supervision of workforce members
- [ ] Established workforce clearance procedures
- [ ] Created termination procedures for ending access to ePHI

### Information Access Management

- [ ] Implemented access authorization procedures
- [ ] Created access establishment and modification procedures
- [ ] Established role-based access controls (RBAC)

### Security Awareness and Training

- [ ] Provided security reminders to workforce members
- [ ] Conducted protection from malicious software training
- [ ] Implemented log-in monitoring procedures
- [ ] Established password management training

### Security Incident Procedures

- [ ] Created incident response and reporting procedures
- [ ] Established incident documentation requirements
- [ ] Defined escalation procedures for security incidents

### Contingency Plan

- [ ] Developed data backup plan
- [ ] Created disaster recovery plan
- [ ] Established emergency mode operation plan
- [ ] Documented applications and data criticality analysis

### Business Associate Agreements

- [ ] Identified all business associates who will access PHI
- [ ] Executed Business Associate Agreements (BAAs) with all partners
- [ ] Documented business associate compliance monitoring procedures

# Physical Safeguards

## Facility Access Controls

- [ ] Implemented contingency operations for facility access
- [ ] Established facility security plan
- [ ] Created access control and validation procedures
- [ ] Implemented maintenance records for facility security

## Workstation and Device Security

- [ ] Defined workstation use policies
- [ ] Implemented workstation security measures (locks, privacy screens)
- [ ] Established device and media controls
- [ ] Created disposal procedures for devices containing ePHI

## Device and Media Controls

- [ ] Implemented media disposal procedures
- [ ] Established media re-use procedures
- [ ] Created accountability procedures for hardware movement
- [ ] Documented data backup and storage procedures

# Technical Safeguards

## Access Control

- [ ] Implemented unique user identification
- [ ] Established emergency access procedures
- [ ] Created automatic logoff procedures
- [ ] Implemented encryption and decryption mechanisms

## Audit Controls

- [ ] Implemented hardware, software, and procedural mechanisms to record and examine access
- [ ] Established audit log review procedures
- [ ] Created audit trail retention policies

## Integrity Controls

- [ ] Implemented mechanisms to authenticate ePHI
- [ ] Established procedures to detect unauthorized alterations
- [ ] Created data integrity validation procedures

## Person or Entity Authentication

- [ ] Implemented procedures to verify identity of persons/entities accessing ePHI
- [ ] Established multi-factor authentication where appropriate
- [ ] Created identity proofing procedures

### Transmission Security

- [ ] Implemented integrity controls for ePHI transmission
- [ ] Established encryption protocols (TLS 1.3 or higher)
- [ ] Created secure transmission procedures and policies

## Privacy Rule Compliance

### Notice of Privacy Practices

- [ ] Created Notice of Privacy Practices (NPP)
- [ ] Established procedures for distributing NPP to patients
- [ ] Implemented acknowledgment of receipt procedures

### Patient Rights

- [ ] Established procedures for patients to access their PHI
- [ ] Created procedures for patients to request amendments to their PHI
- [ ] Implemented accounting of disclosures procedures
- [ ] Established procedures for patients to request restrictions on uses/disclosures
- [ ] Created procedures for patients to request confidential communications

### Uses and Disclosures

- [ ] Limited uses and disclosures to minimum necessary
- [ ] Obtained patient authorization for uses/disclosures not otherwise permitted
- [ ] Established procedures for de-identification of data
- [ ] Created limited data set procedures and data use agreements

### Marketing and Fundraising

- [ ] Established procedures requiring authorization for marketing
- [ ] Created opt-out procedures for fundraising communications

## AI-Specific Considerations

### Algorithm Transparency

- [ ] Documented how AI algorithms use PHI
- [ ] Created plain-language explanations of AI decision-making
- [ ] Established procedures for patients to understand AI-assisted decisions

### Model Training and Testing

- [ ] Ensured training data is properly de-identified or authorized
- [ ] Implemented procedures to prevent re-identification through model outputs
- [ ] Created testing procedures that maintain PHI confidentiality

### Automated Decision-Making

- [ ] Established human oversight for AI-assisted clinical decisions
- [ ] Created procedures for patients to request human review
- [ ] Implemented audit trails for AI decisions involving PHI

### Data Minimization

- [ ] Limited AI access to minimum necessary PHI
- [ ] Implemented data retention and destruction policies for AI training
- [ ] Created procedures for synthetic data use where appropriate

## Documentation and Policies

### Required Policies

- [ ] Privacy Policy
- [ ] Security Policy
- [ ] Breach Notification Policy
- [ ] Data Retention and Destruction Policy
- [ ] Incident Response Policy
- [ ] Access Control Policy
- [ ] Encryption Policy
- [ ] Training Policy

### Documentation Requirements

- [ ] Maintained documentation of all HIPAA compliance activities
- [ ] Established document retention period (6 years from creation or last effective date)
- [ ] Created procedures for updating policies and procedures

## Breach Notification

### Breach Assessment

- [ ] Established procedures to assess potential breaches
- [ ] Created breach risk assessment methodology
- [ ] Implemented breach documentation procedures

### Notification Procedures

- [ ] Established procedures to notify individuals within 60 days
- [ ] Created procedures to notify HHS (within 60 days or annually)
- [ ] Implemented procedures to notify media if breach affects 500+ individuals
- [ ] Documented business associate breach notification procedures

## Monitoring and Auditing

### Regular Reviews

- [ ] Schedule quarterly security risk assessments
- [ ] Conduct annual privacy and security policy reviews

- [ ] Perform periodic workforce compliance audits
- [ ] Review and update this checklist annually

### Compliance Metrics

- [ ] Track number of access attempts and denials
- [ ] Monitor breach incidents and response times
- [ ] Measure training completion rates
- [ ] Document policy update frequency

## Sign-off

**Privacy Officer**: _____ Date: _____

**Security Officer**: _____ Date: _____

**Compliance Officer**: _____ Date: _____

**Project Lead**: _____ Date: _____

---

*This checklist is for educational purposes and should be customized to your specific organization and project requirements. Consult with legal counsel and compliance professionals for comprehensive HIPAA compliance.*