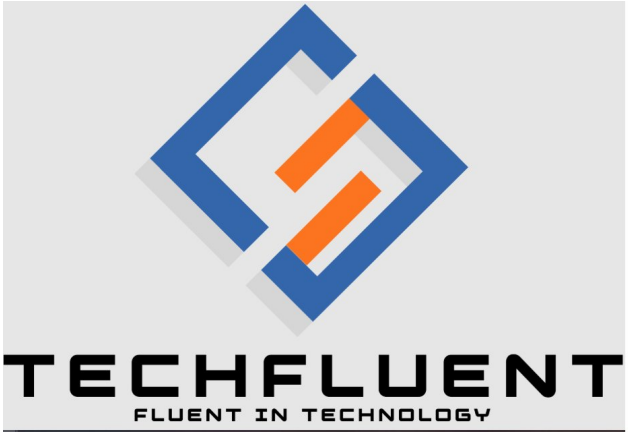


# HIPAA Compliance Checklist

For Healthcare Providers & Medical Practices

**Tech Fluent Pro** | Houston, Texas | www.techfluentpro.com

## About This Checklist

This comprehensive HIPAA compliance checklist is designed to help healthcare providers, medical practices, clinics, and healthcare facilities assess their compliance with the Health Insurance Portability and Accountability Act (HIPAA). Use this checklist to identify gaps in your security and privacy programs and ensure you meet all federal requirements.

**Important:** This checklist provides general guidance and is not a substitute for professional compliance consultation. Healthcare organizations have unique compliance needs based on their size, services, and technology infrastructure. Contact Tech Fluent Pro for a comprehensive HIPAA risk assessment tailored to your practice.

# I. Administrative Safeguards

Administrative safeguards are policies and procedures designed to manage the selection, development, implementation, and maintenance of security measures to protect ePHI.

## A. Security Management Process

- Conducted an accurate and thorough annual Security Risk Analysis (SRA)
- Implemented risk management procedures to address identified risks
- Established sanction policies for workforce members who violate security policies
- Implemented procedures to regularly review information system activity
- Documented all security risk analysis findings and remediation efforts

## B. Workforce Security

- Implemented procedures for authorization and supervision of workforce members
- Established workforce clearance procedures
- Implemented termination procedures (removing access upon separation)
- Maintain current list of all workforce members with access to ePHI

## C. Information Access Management

- Implemented policies limiting access to ePHI based on job roles
- Established procedures for granting access to ePHI
- Documented access authorization procedures
- Regular review and modification of access rights

## D. Security Awareness and Training

- Provide HIPAA security training to all workforce members
- Conduct annual security awareness training
- Training on malware, phishing, and social engineering threats
- Password management training
- Login monitoring and procedures
- Document all training sessions and maintain records

## E. Security Incident Procedures

- Established procedures to identify and respond to security incidents
- Documented incident response plan
- Procedures for reporting security incidents
- Breach notification procedures in place
- Regular testing of incident response procedures

## F. Contingency Plan

- Data backup plan with regular automated backups
- Disaster recovery plan documented and tested
- Emergency mode operation plan
- Testing and revision procedures for contingency plans
- Applications and data criticality analysis completed

## G. Business Associate Agreements

- Identified all business associates who handle ePHI
- Executed HIPAA-compliant Business Associate Agreements (BAAs) with all vendors
- BAAs include all required provisions per HIPAA regulations
- Regular review and updates of BAAs
- Maintain current inventory of all business associates

# II. Physical Safeguards

Physical safeguards protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

## A. Facility Access Controls

- Implemented facility security plan limiting physical access
- Visitor control procedures (sign-in, badges, escorts)
- Access controls for areas containing ePHI systems
- Procedures for validating access to facilities
- Maintenance records for facility access controls

## B. Workstation Security

- Policies specify proper workstation functions and physical attributes
- Workstations positioned to minimize unauthorized viewing of ePHI
- Automatic screen locks/timeouts implemented
- Physical barriers or privacy screens where appropriate

## C. Device and Media Controls

- Policies for disposal of hardware and electronic media containing ePHI
- Procedures for removing ePHI before disposal
- Media re-use procedures ensuring ePHI is removed
- Accountability tracking for hardware and media movement
- Data backup procedures before equipment moves

# III. Technical Safeguards

Technical safeguards are technology and related policies that protect ePHI and control access to it.

## A. Access Control

- Unique user identification for all users
- Emergency access procedures documented
- Automatic logoff after period of inactivity
- Encryption and decryption mechanisms for ePHI
- Multi-factor authentication implemented

## B. Audit Controls

- Mechanisms to record and examine system activity
- Audit logs track access to ePHI
- Regular review of audit logs
- Audit logs protected from modification
- Retention policies for audit logs (minimum 6 years recommended)

## C. Integrity Controls

- Policies to ensure ePHI is not improperly altered or destroyed
- Mechanisms to authenticate ePHI
- Electronic signature controls if used
- Data integrity validation procedures

## D. Transmission Security

- Encryption for ePHI transmitted over open networks
- Secure email for transmitting ePHI
- VPN or other encryption for remote access
- Procedures to guard against unauthorized access during transmission
- Network security measures (firewalls, IDS/IPS)

## IV. Organizational Requirements

- Business associate contracts contain HIPAA-required provisions
- Group health plans have appropriate safeguards
- Required disclosures to plan documents completed
- Hybrid entity designations documented if applicable

## V. Policies, Procedures, and Documentation

- All HIPAA policies and procedures documented in writing
- Policies reviewed and updated annually
- Documentation retained for 6 years from creation/last effective date
- Policies accessible to workforce members
- Sanctions policy for violations
- Policy acknowledgment forms signed by all employees

## VI. Privacy Rule Requirements

- Notice of Privacy Practices (NPP) created and distributed
- NPP acknowledgment obtained from patients
- Privacy Officer designated
- Complaint procedures established
- Minimum necessary standard implemented
- Patient rights procedures (access, amendment, accounting)
- Authorization forms compliant with HIPAA
- Procedures for de-identifying PHI if applicable

## VII. Breach Notification Rule

- ■ Breach notification policies and procedures established
- ■ Risk assessment process for potential breaches documented
- ■ Procedures for notifying individuals within 60 days
- ■ Procedures for notifying HHS (Office for Civil Rights)
- ■ Media notification procedures for large breaches (500+ individuals)
- ■ Business associate breach notification procedures
- ■ Breach log maintained

## Next Steps: Achieve Full HIPAA Compliance

If you've identified gaps in your HIPAA compliance after completing this checklist, Tech Fluent Pro can help. Our healthcare IT specialists provide comprehensive HIPAA compliance services including:

- Annual Security Risk Analysis (required by law)
- HIPAA Policy and Procedure Development
- Workforce HIPAA Training Programs
- Technical Safeguard Implementation
- Business Associate Agreement Management
- OCR Audit Preparation and Support
- Ongoing Compliance Monitoring
- Breach Response and Notification Support

**Schedule Your Free HIPAA Risk Assessment**

Contact Tech Fluent Pro today to discuss your compliance needs and receive a customized security assessment.

**Tech Fluent Pro**
Houston, Texas
www.techfluentpro.com

Protecting Patient Data While Powering Your Practice