# HIPAA Website Compliance Checklist

A comprehensive guide to ensuring your website meets HIPAA requirements

## Technical Safeguards

- [ ] SSL/TLS encryption (HTTPS) implemented across entire website
- [ ] Strong encryption for data at rest (AES-256 or equivalent)
- [ ] Secure authentication mechanisms (multi-factor where applicable)
- [ ] Session timeout after 15 minutes of inactivity
- [ ] Automatic logout on browser close

## Access Controls

- [ ] Role-based access control (RBAC) implemented
- [ ] Unique user identification for all system users
- [ ] Emergency access procedures documented
- [ ] Automatic logoff after inactivity period
- [ ] Encryption and decryption mechanisms in place

## Audit Controls

- [ ] Comprehensive logging of PHI access and modifications
- [ ] Regular audit log reviews (at least quarterly)
- [ ] Tamper-proof audit trail system
- [ ] Log retention for minimum 6 years

## Data Integrity

- [ ] Mechanisms to ensure PHI is not improperly altered or destroyed
- [ ] Regular data backup procedures
- [ ] Disaster recovery plan tested annually
- [ ] Data validation on input forms

## Transmission Security

- [ ] End-to-end encryption for PHI transmission
- [ ] Secure file transfer protocols (SFTP, HTTPS)
- [ ] Email encryption for PHI communications
- [ ] VPN for remote access to systems containing PHI