HIPAA Compliance Testing Checklist

TESTFORT

HIPAA Compliance Testing Checklist

Even though no two healthcare-related software products are identical, HIPAA standards apply to all of them and more.

This is why a testing checklist is a good place to start your compliance testing process — you can use it as-is or adapt it to your project specifics.

These are the main activities and focus areas of HIPAA compliance checks.

1. Administrative Safeguards

Access Control & Authorization

- [ ] Ensure role-based access control is implemented
- [ ] Test authentication mechanisms (multi-factor authentication, unique user IDs)
- [ ] Verify emergency access procedures

Security Management

- [ ] Conduct regular risk assessments and audits
- [ ] Test logging and monitoring of system access
- [ ] Ensure security incident response and reporting procedures

Workforce Training & Policies

- [ ] Ensure all staff are trained on HIPAA policies
- [ ] Verify procedures for terminating access upon employee departure

Third-Party Compliance

- [ ] Check Business Associate Agreements with vendors
- [ ] Assess third-party security compliance

2. Physical Safeguards

Facility Access Control

- [ ] Test physical security controls for data centers
- [ ] Verify restricted access to servers

Workstation & Device Security

- [ ] Enforce screen timeout and auto-lock policies
- [ ] Test secure login requirements for workstations

Media & Device Management

- [ ] Ensure secure disposal of storage media containing PHI
- [ ] Verify encryption of portable devices

3. Technical Safeguards

Data Protection & Encryption

- [ ] Verify data encryption at rest and in transit
- [ ] Test secure transmission of PHI (for example, TLS 1.2+ for emails)
- [ ] Ensure automatic logoff for inactive sessions

Audit Controls & Logging

- [ ] Test logging of system activity and PHI access
- [ ] Ensure audit logs cannot be tampered with

Data Integrity & Protection

- [ ] Test for unauthorized PHI modifications
- [ ] Verify data backup and recovery procedures

Secure Communication & Messaging

- [ ] Ensure patient messages and emails are encrypted
- [ ] Test secure APIs for third-party integrations

4. Privacy Rule Compliance

Patient Access & Authorization

- [ ] Verify patient access to their health records
- [ ] Test electronic consent management systems

Minimum Necessary Rule

- [ ] Ensure only necessary data is accessible to each user
- [ ] Test automatic PHI redaction for non-essential access

De-identification & Anonymization

- [ ] Validate PHI de-identification methods comply with HIPAA standards
- [ ] Ensure anonymized data cannot be re-identified

5. Security Testing

Penetration Testing & Vulnerability Scans

- [ ] Conduct regular penetration testing on EHR infrastructure
- [ ] Test for SQL injection, XSS, and other security vulnerabilities

Incident Response & Breach Notification

- [ ] Test breach detection and response workflows
- [ ] Verify compliance with the 60-day breach notification rule

Backup & Disaster Recovery

- [ ] Ensure data backup policies comply with HIPAA requirements
- [ ] Ensure data backup policies comply with HIPAA requirements

6. Privacy Rule Compliance

Policy & Procedure Documentation

- [ ] Maintain updated policies for HIPAA compliance
- [ ] Review security logs and compliance reports regularly

Compliance Audit & Review

- [ ] Conduct annual HIPAA compliance audits
- [ ] Test staff awareness with security training assessments