HIPAA Compliance Checklist

The following points have been identified by the HIPAA Journal as the components of an effective HIPAA compliance program.

You can use this checklist to self-evaluate your organization.

When you're undergoing a review, you'll be asked the following questions about the handling of your data:

- ☐ Who has access to the data?
- ☐ When did authorized personnel access the data and how?
- ☐ What happens if your company experiences a data breach?
- ☐ How are employees given access to the data?
- ☐ How is permission revoked?
- ☐ How is the data protected?

We've given you an extensive checklist below, but at a high level, here are the boxes you'll need to check to remain HIPAA compliant:

- ☐ Data encryption at rest and in transit
- ☐ Data backups
- ☐ Constant network security
- ☐ Secure tunneling
- ☐ Certificate and key management
- ☐ Compliant internet proxy
- ☐ Audit logging and monitoring

HIPAA requires six annual assessments, and you'll need documentation that proves you have conducted them during the last six years. Make sure you complete the following:

- ☐ Security Risk Assessment
- ☐ Privacy Assessment
- ☐ HITECH Subtitle D Audit
- ☐ Security Standards Audit
- ☐ Asset and Device Audit
- ☐ Physical Site Audit

Here is what you will have to demonstrate:

- ☐ Remediation plans
- ☐ Staff security awareness training
- ☐ ePHI encryption
- ☐ Disposal of PHI and ePHI
- ☐ Emergency contingency plans
- ☐ Staff HIPAA training
- ☐ ePHI access logs
- ☐ Notice of Privacy Practices

Remediation plans

- [ ] Documented plans
- [ ] Gaps and deficiencies list
- [ ] Annual review and update scheduled
- [ ] Remediation plans documented over six years

ePHI encryption

- [ ] Assessment of need for encryption
- [ ] Alternative and equivalent measures in lieu of encryption
- [ ] Documentation of decision regarding encryption

Staff security awareness training

- [ ] Record of security awareness training for each employee
- [ ] Annual security awareness training reminders for staff

Emergency contingency plans

- [ ] Emergency policies and procedures
- [ ] ePHI backups for recovery
- [ ] Contingency plan tests and updates

Disposal of PHI and ePHI

- [ ] Policies and procedures for disposing of physical PHI when it's no longer needed
- [ ] Policies and procedures for permanent deletion of ePHI
- [ ] Secure interim storage of ePHI and physical PHI until permanent deletion and disposal

ePHI access logs

- [ ] Auditable ePHI access logs for successful and unsuccessful login attempts
- [ ] Routine monitoring of ePHI access logs to identify unauthorized access
- [ ] Preventative measures to ensure ePHI integrity

Health information access to patients

- [ ] Access to patient health information when requested by the patient within 30 days of request
- [ ] Reasonable access fees, if charged

Staff HIPAA training

- [ ] Record of annual training for each employee
- [ ] Designated HIPAA compliance organization or staff member

Vendors and business associates

- ☐ Business Associate Agreements (BAAs) with all business associates
- ☐ Due diligence of business associate
- ☐ HIPAA compliance
- ☐ BAA annual tracking
- ☐ Confidentiality agreements with vendors

Notice of Privacy Practices

- ☐ Notice of privacy practices to patients
- ☐ Written statement of receipt from patients
- ☐ Prominent space for notice on website
- ☐ Procedures for complaints about failures to comply

HIPAA authorizations for patients

- ☐ Plain language disclosures and uses of PHI
- ☐ Clear description of people who have access to PHI
- ☐ Authorizations expiry date or event
- ☐ Date and signature of authorization

Security incidents and data breaches

- ☐ Resources to track and manage breach investigations
- ☐ Breach reporting incident procedures
- ☐ Anonymous staff breach reporting mechanisms

Identity management and access controls

- ☐ Unique usernames/numbers for every employee who accesses ePHI
- ☐ Restricted employee access to ePHI on an as needed basis
- ☐ Policies and procedures for assessing ePHI access
- ☐ Policies and procedures for terminating access to ePHI during employee transitions
- ☐ Automatic logout during inactivity integrity

Annual HIPAA Privacy, Security, and Breach Notification Rules

- ☐ Legal attestation of reading from every staff member
- ☐ Annual review documentation

TIP: *For audits, you must provide documentation for the past six years to your auditors. This must include all documentation.*

Please note that the completion of this checklist does not certify HIPAA compliance. These are general questions about the security measures your organization has in place, and should not be taken as legal advice. This checklist has been adapted from the HIPAA Compliance Checklist from the HIPAA Journal.