

HIPAA Compliance Checklist

Health Insurance Portability and Accountability Act • Medical Billing Edition

What is HIPAA? HIPAA is a federal law that protects patients' private health information. Every medical office, billing team, and healthcare provider must follow these rules. Use this checklist regularly to make sure your practice stays compliant and avoids costly fines.

SECTION 1 — Patient Privacy (Privacy Rule)

What To Check		Notes / Reminder
■	Privacy Notice Given to Patients Every new patient gets a written Notice of Privacy Practices (NPP) explaining how their health info is used.	<i>Keep a signed copy on file</i>
■	Minimum Necessary Rule Followed Only share the least amount of patient information needed — never share more than required.	<i>Train all staff on this rule</i>
■	Patient Authorizations in Place If you share records for anything beyond treatment or billing, you have a signed patient authorization form.	<i>Review monthly</i>
■	Patient Rights Honored Patients can request to see, copy, or correct their records. All requests are answered within 30 days.	<i>Log every request</i>
■	Business Associate Agreements (BAA) Signed Any outside company that handles patient data (labs, billing services, IT) has a signed BAA with your office.	<i>Review annually</i>

SECTION 2 — Electronic Data Security (Security Rule)

What To Check		Notes / Reminder
■	Strong Passwords in Use All computers and systems use passwords that are at least 8 characters with numbers and symbols.	<i>Change every 90 days</i>
■	Automatic Screen Lock Enabled Computer screens lock automatically after 5–10 minutes of no activity.	<i>Check all workstations</i>
■	Encrypted Emails for Patient Data Any email containing patient health information is encrypted (scrambled so only the receiver can read it).	<i>Use secure email tools</i>
■	Data Backup Running Patient data is backed up daily to a secure location. Backups are tested to make sure they work.	<i>Test restores quarterly</i>
■	Antivirus & Firewall Active All computers have up-to-date antivirus software and a firewall turned on at all times.	<i>Check update logs</i>

■	Access Controls Set Up Each staff member only has access to the patient data they need for their specific job — no more.	<i>Review access quarterly</i>
■	Audit Logs Reviewed System logs that track who accessed patient records are reviewed regularly for anything unusual.	<i>Review monthly</i>

SECTION 3 — Physical Security

What To Check		Notes / Reminder
■	Paper Records Secured All printed patient records are kept in locked cabinets. Only authorized staff can access them.	<i>Use key sign-out log</i>
■	Visitor Sign-In Required Any outside person entering the office must sign in. No one gets into patient data areas unescorted.	<i>Keep visitor log</i>
■	Documents Shredded Properly Old patient papers are shredded with a cross-cut shredder before being thrown away.	<i>Use locked shred bins</i>
■	Device Disposal Policy Followed Old computers, hard drives, and USB drives with patient data are wiped completely before disposal.	<i>Document every disposal</i>
■	Workstations Positioned Carefully Computer screens are not visible to waiting room patients or hallway traffic.	<i>Use privacy screens if needed</i>

SECTION 4 — Breach Response Plan

What To Check		Notes / Reminder
■	Breach Response Plan Written Your office has a written step-by-step plan explaining what to do if patient data is stolen or leaked.	<i>Review every 6 months</i>
■	Staff Know How to Report a Breach Every team member knows exactly who to call and what to do if they suspect a data breach.	<i>Include in training</i>
■	Breach Notification Timelines Known Staff know that patients must be notified within 60 days of discovering a breach.	<i>Post reminder in office</i>
■	Incidents Logged Any small security incident — even if not a full breach — is recorded in a written incident log.	<i>Keep log for 6 years</i>

SECTION 5 — Staff Training

What To Check		Notes / Reminder
■	Annual HIPAA Training Completed All staff complete HIPAA training at least once a year. New hires are trained before starting work.	<i>Save training certificates</i>

■	Training Records on File You have written proof that every staff member completed their HIPAA training.	<i>Keep for 6 years</i>
■	Sanctions Policy Exists There is a written policy explaining what happens if a staff member violates HIPAA rules.	<i>Include in employee handbook</i>
■	Policies Updated Regularly Your HIPAA privacy and security policies are reviewed and updated whenever laws change or yearly.	<i>Date-stamp all updates</i>

■ **Important Reminder:** HIPAA violations can result in fines from \$100 to \$50,000 per violation. Criminal violations can lead to jail time. Completing this checklist regularly protects your patients, your staff, and your practice.