



HIPAA-Compliance Checklist for Therapists

Any therapist running their own practice should be prepared to invest time, energy, and cash making sure their business is 100% in compliance with HIPAA.

Here's a quick checklist of items you need to address, whether you're setting up shop for the first time or doing a periodic audit of your HIPAA practices.

For an in-depth guide, see [HIPAA Journal's Official HIPAA Compliance Checklist](#).

Physical HIPAA safeguards for therapy practices

- In-person access to records**
Any paper records of your clients' health information must be protected from access. That may include a lockable take-home file box for patient notes, and locks or other security measures to protect your office from unwanted access.
- Dedicated work computers**
If sensitive information is stored locally on a computer, make sure it's used for business purposes only.
- Protected work computers**
Any computer storing sensitive information should only be accessible by qualified staff.
- Physical media management**
Keep an inventory of any physical media used to store digital files (eg. USB keys, portable hard drives). Restrict access to these media, and ensure they're reformatted or disposed of correctly when no longer needed.

Technical HIPAA safeguards for therapy practices

- Access control**
Protect your clients' privacy by controlling who has login information for local and cloud-based storage, as well as implementing automatic logoff procedures and encryption when appropriate.
- Integrity control**
Any system you use to store notes, patient files, or other sensitive information should be able to record and report when changes are made.
- Person or entity identification**
Use tools like two-factor authentication, face or fingerprint scanning, etc. to restrict access to work computers and sensitive files.
- Transmission security**
Any system being used to transmit patient information should be encrypted. Electronic health record (EHR) and payment software must be HIPAA-compliant.