HIPAA COMPLIANCE CHECKLIST

This document is not a substitute for legal advice or consultation, or a substitute for clinical or ethical consultation or advice. These checklists are for reference only. Consult with your attorney, licensing organization, and professional code of ethics prior to use. Additionally, we suggest you have your legal counsel review and approve all of your practice's HIPAA-related policies, consent forms, office procedures, and risk assessments.

☐ **Share your Notice of Privacy Practices policy**

- Post an updated "Notice of Privacy Practices" (NOPP) policy in your office that is compliant with current HIPAA rules.
- Offer all new clients a copy of your updated NOPP. For existing clients, post on your website, or distribute directly.

☐ **Review your state-specific HIPAA requirements**

Most states have specific additions or revisions that provide more protection to clients than federal HIPAA guidelines. This can include expanded definitions, required training expectations for new therapists, and client access to records. Visit your state's department of public health, department of human services, or health office of compliance and technology for details.

☐ **Make sure you have all of the HIPAA-compliant forms you need for your practice**

These may include:

- NOPP form
- Risk Assessment
- Informed Consent
- Email Consent
- Consent to Release Form
- Business Associate Policy
- Business Associate Form
- Breach Policy
- Breach Notification Log
- Complaints Log
- Disclosure Log
- Ongoing Compliance Review Log
- Policies & Procedures document

☐ **Perform a HIPAA-compliant risk assessment**

- **Conduct a risk assessment for privacy and security breaches, including an inventory of electronic devices containing client Protected Health Information (PHI)**. Identify all of the places your clients' PHI is located where privacy and security might be at risk.

- Common places include your computer, cell phone, email; paper files and file cabinets; your digital copier/printer's hard drive; deleted computer files; and even your website's contact form.

- **Make a risk management response plan that meets both the HIPAA Security standards and your own security needs**. Ask yourself: What could go wrong? What is the likelihood of that happening? What problems would it cause for my clients and my practice?

  Your risk assessment should include:
  - Potential risks
  - Current security/privacy protocols
  - Likelihood of a breach
  - Potential impact of a breach
  - Prioritization of high risk or high impact issues
  - Plans and timeline to address those risks
  - Progress made/ date fixed

- **Maintain documentation of all assessments, plans, actions, and resources in a safe place.** Update these documents annually if possible.

- **Understand what constitutes a breach, and what your responsibilities are, if there ever is one.** The action steps vary, depending on the size of the breach. Also understand your obligations for client disclosures and HIPAA complaints.

☐ **Protect your practice and your clients**

- Appoint a "Privacy Officer" and/or "Security Officer" for your practice (which can be yourself). This person would also be responsible for updating his/her HIPAA training regularly.

- Have a disaster recovery plan. Designate a person to put a contingency plan in place in case you are sick, incapacitated, or die. Document this plan and share with that person.

- Use strong passwords, virus protection, and a firewall for all of your electronic devices. Consider consulting with an IT professional to identify areas of vulnerability.

- Request signed Business Associate Agreements (BAAs) from your vendors and service providers, employees, cloud storage providers, and other businesses that have access to your clients' PHI.

☐ **Research HIPAA-compliant business tools**

- Tools may include a cloud-based practice management system allows you to keep stored PHI off your own devices, lowering your tech risks.

- Make sure that whatever service you use for your practice provides a BAA.
- Remember that a product cannot make you "HIPAA compliant."

☐ **Check out these suggested resources**

HIPAA Resources, U.S. Department of Health & Human Services
https://www.hhs.gov/hipaa/index.html

- ***HIPAA Training***
  https://www.hhs.gov/hipaa/for-professionals/training/index.html

HIPAA and Preemption of State Law
https://www.hhs.gov/hipaa/for-professionals/faq/preemption-of-state-law/index.html

Information on Breaches
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HIPAA for Therapists free resources
https://hipaafortherapists.com/category/free-resources/

Person-Centered Tech free articles
https://personcenteredtech.com/articles/collections/

Review of practice management software from American Psychological Association: "How Does This Practice Management Software Stack Up?"
https://www.apaservices.org/practice/business/technology/tech-column/practice-management-software

Recommended technology, tools, and resources for therapists and counselors (from TameYourPractice.com)
https://www.tameyourpractice.com/blog/recommended-technology-tools-resources-for-therapists/