## HIPAA Risk Assessment Checklist for Small Practices

This checklist is designed to help solo practitioners and small healthcare practices assess their compliance with HIPAA privacy and security requirements. Use it to identify gaps and develop an action plan.

### 1. Administrative Safeguards

- ☐ Have you designated a Privacy and Security Officer (can be the same person)?
- ☐ Do you have written HIPAA policies and procedures?
- ☐ Do you provide HIPAA training to all staff (or document your own self-training)?
- ☐ Do you have Business Associate Agreements (BAAs) in place with vendors who handle PHI?
- ☐ Have you conducted a HIPAA risk assessment in the past year?
- ☐ Do you have a process to review and update HIPAA policies regularly?

### 2. Physical Safeguards

- ☐ Are paper records stored in a locked file cabinet or secure room?
- ☐ Are workstations and devices used to access PHI physically secure?
- ☐ Are mobile devices encrypted and protected with passcodes?
- ☐ Do you properly dispose of paper and electronic records (e.g., shredding, wiping drives)?

### 3. Technical Safeguards

- ☐ Are electronic systems password-protected and encrypted?
- ☐ Do you use secure, HIPAA-compliant email or messaging platforms for client communication?
- ☐ Are audit logs enabled on your EHR system (if applicable)?
- ☐ Do you regularly back up electronic records in a secure manner?
- ☐ Do you update software and security patches regularly?

### 4. Breach Notification and Response

- ☐ Do you have a written breach response plan?
- ☐ Do you know how to assess and document a potential breach?
- ☐ Are you prepared to notify affected clients and HHS in case of a breach?
- ☐ Do you maintain a breach log and retain it for 6 years?

### 5. Client Rights and Communication

- ☐ Do you provide a Notice of Privacy Practices to each client?
- ☐ Can clients access and request changes to their health records?
- ☐ Do you have a process for responding to client privacy complaints?