PRACTICE RESOURCE

HIPAA Compliance Checklist

A practical, plain-language checklist for psychologists, therapists, counselors, and behavioral health practices.

Start with a Security Risk Analysis (SRA)
A documented, organization-wide SRA is the foundation of HIPAA compliance — and the single most commonly cited deficiency in OCR enforcement. Use this checklist to track your safeguards, then revisit it after any major change. Check each box as you confirm it is implemented *and* documented.

1. Program Foundations

45 CFR §164.530 · §164.308 · §164.316

- [ ] **Appoint a Privacy Officer and a Security Officer** §164.530(a) · §164.308(a)(2)
  Name accountable individuals responsible for developing and enforcing your HIPAA program.
- [ ] **Complete a documented Security Risk Analysis** §164.308(a)(1)(ii)(A)
  Identify where ePHI lives and assess risks to its confidentiality, integrity, and availability. The free HHS SRA Tool is a good starting point.
- [ ] **Adopt written policies and procedures** §164.316(a) · §164.530(i)
  Maintain current, practice-specific HIPAA policies — not generic templates left unread on a shelf.
- [ ] **Implement a risk management plan** §164.308(a)(1)(ii)(B)
  Prioritize and remediate the gaps your risk analysis uncovers, and track them to closure.
- [ ] **Maintain a workforce sanction policy** §164.308(a)(1)(ii)(C)
  Define consequences for staff who violate privacy or security rules, and apply them consistently.
- [ ] **Retain documentation for at least six years** §164.316(b)(2) · §164.530(j)
  Keep policies, risk analyses, training logs, and incident records for six years from creation or last effective date.

2. Administrative Safeguards

45 CFR §164.308

- [ ] **Authorize and supervise workforce access** §164.308(a)(3)
  Grant ePHI access based on job role, and supervise staff who work with protected information.
- [ ] **Terminate access promptly on departure** §164.308(a)(3)(ii)(C)
  Revoke logins, keys, and devices immediately when a workforce member leaves or changes roles.
- [ ] **Apply role-based information access management** §164.308(a)(4)
  Limit each user to the minimum systems and records their role requires.
- [ ] **Deliver ongoing security awareness training** §164.308(a)(5)
  Cover phishing, malware, password hygiene, and reporting — with periodic reminders.
- [ ] **Establish security incident procedures** §164.308(a)(6)
  Define how staff identify, report, respond to, and document suspected security incidents.
- [ ] **Maintain a contingency plan** §164.308(a)(7)
  Include data backup, disaster recovery, and emergency-mode operation so care continues during an outage.

- [ ] **Review information system activity** §164.308(a)(1)(ii)(D)
  Routinely review audit logs, access reports, and security incident tracking.
- [ ] **Perform periodic evaluations** §164.308(a)(8)
  Re-assess your safeguards in response to operational or environmental changes.

3. Physical Safeguards

45 CFR §164.310

- [ ] **Control facility access** §164.310(a)(1)
  Limit physical entry to areas housing ePHI with locks, badges, or visitor sign-in.
- [ ] **Govern workstation use and placement** §164.310(b)
  Position screens away from waiting areas and public sightlines; define acceptable use.
- [ ] **Physically secure workstations and devices** §164.310(c)
  Lock or restrain devices and enforce screen locks when unattended.
- [ ] **Manage devices and media end-to-end** §164.310(d)(1)
  Track, securely wipe, and properly dispose of drives, phones, and paper containing ePHI.
- [ ] **Store backups securely and encrypted** §164.310(d)(2)(iv)
  Keep recoverable, encrypted copies of ePHI, ideally offsite or in a vetted cloud.

4. Technical Safeguards

45 CFR §164.312

- [ ] **Assign unique user IDs** §164.312(a)(2)(i)
  Give every workforce member their own login — never shared accounts — for traceability.
- [ ] **Enable automatic logoff / session timeout** §164.312(a)(2)(iii)
  End inactive sessions automatically so unattended screens don't expose ePHI.
- [ ] **Encrypt ePHI at rest and in transit** §164.312(a)(2)(iv) · (e)(2)(ii)
  Encrypt stored data and any ePHI sent over networks; encryption is your safe harbor in a breach.
- [ ] **Require multi-factor authentication** §164.312(d)
  Verify identity with MFA for email, EHR, and remote access to systems holding ePHI.
- [ ] **Maintain audit controls and logging** §164.312(b)
  Record and retain who accessed what, and when, across systems that touch ePHI.
- [ ] **Protect data integrity** §164.312(c)(1)
  Guard against improper alteration or destruction of ePHI.
- [ ] **Secure transmissions** §164.312(e)(1)
  Use secure email, portals, or encrypted messaging — not standard email — for PHI.
- [ ] **Maintain anti-malware / endpoint protection** §164.308(a)(5)(ii)(B)
  Keep endpoint security active and updated on every device that handles ePHI.

5. Privacy Rule Essentials

45 CFR §164.500 et seq.

- [ ] **Provide a Notice of Privacy Practices** §164.520
  Give patients a current NPP and post it where they can see it, including online.
- [ ] **Apply the minimum necessary standard** §164.502(b) · §164.514(d)
  Use or disclose only the least PHI needed for the task at hand.
- [ ] **Honor patient access requests** §164.524
  Provide records, generally within 30 days, in the form and format the patient requests when feasible.

- [ ] **Process amendment requests** §164.526
  Let patients request corrections to their records and respond within the required timeframe.
- [ ] **Maintain an accounting of disclosures** §164.528
  Track disclosures that fall outside treatment, payment, and operations.
- [ ] **Obtain valid authorizations when required** §164.508
  Get written, HIPAA-compliant authorization for uses and disclosures not otherwise permitted.
- [ ] **Offer restrictions and confidential communications** §164.522
  Accommodate reasonable requests for restricted use or alternative contact methods.

6. Behavioral & Mental Health Specifics

45 CFR §164.508 · 42 CFR Part 2 · State law

- [ ] **Protect psychotherapy notes separately** §164.508(a)(2)
  Keep process notes apart from the chart; most disclosures require a separate, specific authorization.
- [ ] **Apply 42 CFR Part 2 to SUD records** 42 CFR Part 2
  Substance use disorder records from covered programs carry stricter consent rules than HIPAA alone.
- [ ] **Follow stricter state laws** NY Mental Hygiene Law · SHIELD Act
  Where state law is more protective than HIPAA, the stricter standard applies.
- [ ] **Use only BAA-covered telehealth platforms** §164.502(e)
  Confirm your video and messaging tools are HIPAA-eligible and backed by a signed BAA.
- [ ] **Watch for "logical deduction" PHI exposure** §164.514(b)
  Pairing a name or contact with a behavioral health provider's identity can itself reveal PHI — even without clinical detail.

7. Business Associates & Vendors

45 CFR §164.308(b) · §164.502(e) · §164.504(e)

- [ ] **Sign a BAA with every business associate** §164.502(e)(1)
  Any vendor that creates, receives, maintains, or transmits ePHI on your behalf needs a signed BAA.
- [ ] **Confirm BAAs contain the required terms** §164.504(e)
  Verify each agreement addresses permitted uses, safeguards, breach reporting, and termination.
- [ ] **Perform vendor due diligence** §164.308(a)(1)
  Vet EHR, billing, scheduling, email, cloud, and IT/MSP vendors before sharing ePHI.
- [ ] **Verify your plan tier is BAA-eligible** Vendor BAA
  Some email and cloud services (e.g., certain Microsoft 365 tiers) only offer a BAA on qualifying plans.
- [ ] **Keep a current ePHI vendor inventory** §164.308(a)(1)
  Maintain a living list of every tool and partner that handles ePHI, with BAA status.

8. Breach Readiness & Response

45 CFR §§164.400–414

- [ ] **Maintain a written breach response plan** §164.414(a)
  Document who does what, and how fast, the moment a possible breach is detected.
- [ ] **Run the four-factor risk assessment** §164.402
  Assess each incident to determine whether a reportable breach has occurred.
- [ ] **Notify affected individuals within 60 days** §164.404
  Send individual notice without unreasonable delay and no later than 60 days from discovery.
- [ ] **Report to HHS OCR on the required timeline** §164.408
  Breaches affecting 500+ individuals are reported within 60 days; smaller breaches are logged and reported annually.

- [ ] **Provide media notice for large breaches** §164.406
  Notify prominent media when a breach affects more than 500 residents of a state or jurisdiction.
- [ ] **Require BAs to report breaches to you** §164.410
  Your BAAs should obligate associates to notify you promptly so your clock can start.

9. Training & Ongoing Maintenance

45 CFR §164.530(b) · §164.308(a)(5) · §164.316

- [ ] **Train every workforce member at onboarding** §164.530(b)
  Provide HIPAA training to all staff, including new hires, before they handle PHI.
- [ ] **Refresh training periodically and after changes** §164.308(a)(5)
  Repeat training on a regular cadence and whenever policies, systems, or threats change.
- [ ] **Re-run the SRA at least annually** §164.308(a)(1)
  Update your risk analysis yearly and after any significant operational change.
- [ ] **Review and update policies regularly** §164.316(b)(2)(iii)
  Keep documentation current as your practice, vendors, and regulations evolve.
- [ ] **Document training and program activity** §164.530(j)
  Keep dated records of training completion and compliance work to demonstrate good-faith effort.

Ready to Simplify HIPAA Compliance?

Let's build a safer, more confident practice — together. Reach out for a free consultation.

CALL **631-388-4274**

EMAIL **support@a1plusai.com**

WEBSITE **a1plusai.com**

SERVING **New York & Long Island**