The Complete HIPAA Compliance Documentation Kit for Therapists

Security Risk Assessment · BAA Request Letter · Notice of Privacy Practices
Telehealth Consent · Breach Notification Procedure · State Law Reference

Prepared by Therapy HIPAA Hub — therapyhipaahub.com
Edition: November 2026

How to Use This Kit

This kit is a set of editable templates and checklists, not a substitute for legal advice. Every template here reflects the same facts we publish and keep current on therapyhipaahub.com — fill in your practice's details, adapt the language to your situation, and keep a copy of everything you complete for at least 6 years, which is the HIPAA documentation retention standard.

This kit covers federal HIPAA requirements that apply everywhere in the US, plus a state-law quick-reference appendix for the states most of our readers practice in. If your state isn't listed, check the latest version of our city-specific guides at therapyhipaahub.com/compliance/ for ongoing updates.

This is not legal advice, and purchasing this kit does not create an attorney-client or consulting relationship. For your specific situation, especially anything involving an active OCR complaint or audit, consult a healthcare attorney licensed in your state.

1. Security Risk Assessment (SRA) — Full Checklist

The HIPAA Security Rule requires every covered entity to conduct and document a Security Risk Assessment. This is the single most commonly missing document in OCR audits. Work through all four categories below, mark each item, and keep this completed checklist on file.

Administrative Safeguards

- ☐ Designated Privacy Officer and Security Officer (can be the same person in a solo practice)
- ☐ Written policies for who can access client records, and under what circumstances
- ☐ Documented HIPAA training completed by you and any staff, with dates
- ☐ Sanction policy describing what happens if staff violate HIPAA policy
- ☐ Documented process for terminating access when a staff member or contractor leaves
- ☐ Annual review date for this entire Security Risk Assessment

Physical Safeguards

- ☐ Workstations with access to PHI are positioned so screens aren't visible to unauthorized people
- ☐ Physical files containing PHI are stored in a locked location when not in use
- ☐ Documented policy for secure disposal of physical records (shredding, not trash)
- ☐ Device inventory: every laptop, tablet, and phone that can access PHI is logged
- ☐ Plan for what happens to devices when they are retired, lost, or stolen

Technical Safeguards

- ☐ Multi-factor authentication (MFA) enabled on all accounts with PHI access (EHR, email, cloud storage)
- ☐ Encryption at rest and in transit for all systems storing PHI
- ☐ Automatic logoff or screen lock after a period of inactivity on all devices
- ☐ Audit logs available for who accessed which client records and when
- ☐ Firewall and up-to-date antivirus/anti-malware on all devices touching PHI
- ☐ Documented backup procedure, with backups tested at least annually

Organizational Requirements

- ☐ Signed Business Associate Agreements (BAAs) on file for every vendor touching PHI (EHR, email, telehealth, scheduling, billing, cloud storage)
- ☐ Written Breach Notification Policy (template in Section 5 of this kit)
- ☐ Current, signed Notice of Privacy Practices (template in Section 3)

• Documented data retention and destruction policy consistent with your state's requirements

Documentation requirement: completing this checklist alone is not sufficient. For each unchecked item, write down (1) the specific risk, (2) your remediation plan, and (3) your target completion date. Keep this written record — it is what OCR auditors ask for first.

2. BAA Request Letter Template

Send this to any vendor that creates, receives, maintains, or transmits PHI on your behalf and does not already have a signed Business Associate Agreement with you.

[Your Practice Name]

[Your Address]

[Date]

[Vendor Name]

Attn: Privacy/Compliance Officer

Re: Business Associate Agreement Request

Dear [Vendor Name],

Our practice uses [Vendor Name/Product] in a capacity that involves creating, receiving, maintaining, or transmitting Protected Health Information (PHI) on our behalf. Under the HIPAA Privacy and Security Rules, this makes [Vendor Name] a “Business Associate,” and a signed Business Associate Agreement (BAA) is required before we can continue using your service with client data.

Please provide your standard BAA for review and signature, or confirm you can execute the HHS model BAA (available at hhs.gov). If your organization does not currently offer a BAA, please let us know by [date two weeks out] so we can evaluate alternative vendors.

Thank you for your prompt attention to this compliance requirement.

Sincerely,

[Your Name]

[Your Practice Name]

[Your Phone/Email]

Tip: send by email with a read receipt, or certified mail if a vendor has gone unresponsive — a documented request date matters if OCR ever asks what steps you took.

3. Notice of Privacy Practices (NPP) — Template

Give this to every new client at first service, post it in your office and on your website, and have clients sign an acknowledgment of receipt.

Accuracy note: most of the 2024 federal reproductive-health-specific NPP provisions were vacated by a federal court in June 2025. What remains with a February 16, 2026 compliance deadline is narrower — specific to substance use disorder (42 CFR Part 2) records. This template reflects the core NPP language that applies to every covered entity, without the vacated language. If you handle Part 2-covered records, confirm current Part 2-specific NPP requirements with a healthcare attorney.

Notice of Privacy Practices
[Your Practice Name]
Effective Date: [Date]

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Our Commitment to Your Privacy: We are required by law to maintain the privacy of your protected health information (PHI) and to provide you with this notice of our legal duties and privacy practices.

How We May Use and Disclose Your Information: We may use and disclose your PHI for treatment, payment, and healthcare operations. Examples include coordinating your care with other providers, billing your insurance, and internal quality review. We will not use or disclose your psychotherapy notes without your specific written authorization, except in limited circumstances required by law (for example, to avert a serious threat to health or safety, or in response to a court order).

Your Rights: You have the right to request restrictions on certain uses and disclosures, to request confidential communications, to inspect and copy your record (with some exceptions for psychotherapy notes), to request amendment of your record, to receive an accounting of certain disclosures, and to receive a paper copy of this notice upon request.

Changes to This Notice: We reserve the right to change this notice and to make the new notice provisions effective for all PHI we maintain. The current notice is available at our office and on our website.

Complaints: If you believe your privacy rights have been violated, you may file a complaint with our practice and with the Secretary of the U.S. Department of Health and Human Services. You will not be retaliated against for filing a complaint.

Contact: [Your Name / Privacy Officer], [Phone], [Email]

Acknowledgment of Receipt
I acknowledge that I have received a copy of this Notice of Privacy Practices.

Client signature: _____ Date: _____

4. Telehealth Informed Consent Template

HIPAA requires informed consent before the first telehealth session. Several states add their own specific requirements — check the state appendix in Section 6.

A complete telehealth consent should include:

- Description of the telehealth technology used and its general limitations
- Explanation of the HIPAA protections in place and the potential risks of telehealth versus in-person care
- Your right to stop telehealth and switch to in-person sessions at any time
- Emergency procedures if the connection fails or if you are in crisis during a session
- Confirmation that you are in a private location for the session
- Your current physical location at the start of the session (required in some states for licensing purposes)
- Confirmation of which state you are physically located in, so your therapist can confirm they are licensed to treat you there

Client Acknowledgment: I have read and understand the above. I consent to receive therapy services via telehealth.

Client signature: _____ Date: _____

5. Breach Notification Procedure Template

HIPAA requires a written breach notification procedure as part of your Organizational Requirements. Adapt the timeline below to any stricter state law deadline that applies to you (see Section 6).

Step 1 — Identify and contain. The moment a potential breach is discovered, document the date, what happened, and what PHI may have been exposed. Contain the exposure immediately (revoke access, change passwords, retrieve lost devices if possible).

Step 2 — Assess. Determine whether the incident meets HIPAA's definition of a reportable breach (unauthorized use or disclosure of unsecured PHI) using the four-factor risk assessment: nature of the PHI involved, who received or accessed it, whether it was actually viewed, and the extent the risk was mitigated.

Step 3 — Notify affected individuals. Federal HIPAA requires notification within 60 days of discovery. Some states (for example, California) require notification within as few as 5 business days — check your state's requirement in Section 6 and use whichever deadline is stricter.

Step 4 — Notify HHS. Breaches affecting 500+ individuals must be reported to HHS within 60 days and simultaneously to local media. Breaches affecting fewer than 500 individuals are logged and reported to HHS annually, within 60 days of the end of the calendar year.

Step 5 — Document everything. Keep a breach log (even for near-misses that didn't rise to a reportable breach), your risk assessment, notification letters sent, and remediation steps taken. Retain for 6 years.

6. State Law Quick-Reference Appendix

HIPAA is a federal floor — states can and do require more. This appendix summarizes what adds the most obligation on top of HIPAA in each state below. This is not exhaustive; always confirm current requirements with a licensed attorney in your state.

State	What's Different From Baseline HIPAA
California	CMIA requires breach notification within 5 business days (vs. HIPAA's 60). Prohibits selling medical information in any form. California Board of Behavioral Sciences requires records retention of 7 years for adults, until a minor's 25th birthday.
Texas	Texas Health & Safety Code Chapter 611 governs mental health records specifically and is stricter than HIPAA in several areas. OCR Region 6 (covering Texas) is among the most active federal enforcement regions.
New York	Strong state-level mental health record protections layered on top of HIPAA; psychotherapy notes receive heightened protection under both federal and state frameworks.
Florida	State licensing board (Board of Clinical Social Work, Marriage & Family Therapy, and Mental Health Counseling) maintains its own record-keeping and confidentiality rules independent of OCR.
Illinois	The Mental Health and Developmental Disabilities Confidentiality Act (MHDDCA) provides privacy protections specific to mental health records, including for telehealth, beyond HIPAA's general standard.
Washington	My Health My Data Act (MHMDA), effective March 2024 — the first state law of its kind. Regulates 'consumer health data' more broadly than HIPAA, requires a standalone Consumer Health Data privacy policy and opt-in consent, and uniquely allows a private right of action (clients can sue directly), with penalties up to $7,500 per violation.
Colorado	Mandatory written disclosure to clients at initial contact, updated effective August 1, 2024, separate from the HIPAA NPP. Treatment records may not be retained beyond 7 years under state statute — a maximum, not just a minimum.
Arizona	A.R.S. § 36-509 makes behavioral health treatment records confidential and not public record. The Arizona Board of Behavioral Health Examiners can independently investigate confidentiality complaints, separate from any federal OCR action.

For the most current version of this appendix, including additional states and any legal updates since this edition, see therapyhipaahub.com/compliance/

Questions or Updates

HIPAA guidance and state law change. We update the free guides at therapyhipaahub.com whenever something in this kit changes materially. This kit is a snapshot as of November 2026 — always verify anything high-stakes (a specific state deadline, a specific vendor's current BAA terms) directly before relying on it for an active compliance decision.