

The Compliant AI Workbook for EMDR Therapists

Work through the ten steps, tick each box, and fill in the blanks. When every box is checked, you are using AI the way it is meant to be used.

The one rule everything rests on: **AI drafts. You decide and sign.**

YOUR PRACTICE

CLINICIAN NAME

Full name

LICENSE OR REGISTRATION NUMBER

e.g. LMFT #00000

PRACTICE STATE

e.g. Pennsylvania

DATE STARTED

mm/dd/yyyy

THE TEN STEPS

1

Get a signed BAA for every tool that touches client data

A Business Associate Agreement (BAA) is the contract that makes a vendor **legally responsible** for protecting your clients' data. **No BAA means no PHI goes in.** This applies to every link in the chain, your video platform, your transcription tool, **and** the AI itself.

List your tools and confirm the BAA for each:

TOOL	WHAT IT IS USED FOR	BAA SIGNED? (DATE)
Video platform	Telehealth sessions	Y / N
Transcription	Session recordings	Y / N
AI assistant	Drafting notes	Y / N
EHR or practice system	Records	Y / N
Other		Y / N

WHERE TO ACTUALLY GET THE BAA

ChatGPT and Claude: the plan you need, and how to sign

Here is the part that trips everyone up: **the popular plans cannot be made compliant**. A BAA is only available on the enterprise and developer tiers. Below is exactly which plan carries a BAA, and how to sign it.

ChatGPT (OpenAI)

CONSUMER PLANS: NO BAA

Free • Plus • Team • Business	✗ No BAA available on any of these. Putting client data in is a HIPAA violation, full stop.
ChatGPT Enterprise	✓ BAA available, but only through a sales managed account, so you cannot set it up yourself.
OpenAI API	✓ BAA available if you, or your developer, build on the API directly.
ChatGPT for Healthcare	Launched Jan 2026, genuinely HIPAA capable, but it is an enterprise deployment for health systems , not something a solo practice signs up for like Plus. Note that consumer "ChatGPT Health" will never get a BAA, so do not confuse the two.

How to request it

1. **Enterprise:** you need a sales managed account. Contact OpenAI Sales and ask to add the BAA to your Enterprise workspace.
2. **API:** email baa@openai.com with your company and use case. They typically reply within one or two business days, and review case by case.
3. Sign the BAA **before** any client data goes in. Store your copy.

Claude (Anthropic)

CONSUMER PLANS: NO BAA

Free • Pro • Max • Team	✗ No BAA. These cannot be covered at all, so never put PHI in them.
Claude Enterprise	✓ Offers a HIPAA ready configuration with a click to accept BAA. Available self serve, or sales assisted.
Claude API	✓ BAA available. Your account's Primary Owner signs, then contacts Anthropic to enable it.

How to turn it on (Enterprise, self serve)

1. Be on an **Enterprise** plan. Self serve carries a **20 seat minimum at roughly \$20 per seat per month, billed annually**, so about \$4,800 a year in seat fees, with model usage billed on top.
2. As Primary Owner, go to **Organization settings**, then **Data and privacy**, then **HIPAA compliance**.
3. Click "**Accept and Enable HIPAA.**" That click **is** your acceptance of the BAA, so there is no separate document to mail back.
4. Confirm the checkmark appears in the HIPAA Compliance section. Note that some features are **excluded** from the BAA even once it is on, so check the current exclusion list before you rely on one.

The honest reality check for a solo or small practice

"Just get Enterprise" is technically true and practically brutal: 20 seat minimums, sales calls, and enterprise procurement, all so you can write your progress notes. For most independent EMDR clinicians, standing up ChatGPT Enterprise or Claude Enterprise on your own is not realistic. So you have **two paths that actually work**:

Path A, a purpose built tool

A clinical platform that already signs a BAA without the enterprise overhead, with recording, transcription, anonymization and prompts built in. This is the gap WeMind fills.

Path B, de identified text only

Keep using a general AI, but feed it **only** text with all 18 identifiers stripped, see Step 5. More manual, and one slip is a breach.

Plans, pricing and BAA terms move fast in this space, so always confirm the current terms on the vendor's own compliance page before you sign.

- ☐ Every tool that touches client data will sign, or has signed, a BAA with me.
- ☐ I have stored a copy of each signed BAA where I can find it.
- ☐ I checked what runs under the hood, so my tool is not quietly piping data to a general chatbot with no BAA.

2

Never paste client identifiers into a tool without a BAA

This is the **number one mistake**. The moment identifiable client information lands in consumer ChatGPT, Claude, Gemini or Copilot, you have made an impermissible disclosure. Speed is never worth it.

THE LINE YOU DO NOT CROSS

No names, no dates of birth, no "my client in [town]", nothing that could identify a person, into any tool without a signed BAA.

MY PERSONAL RULE, IN MY OWN WORDS (WRITE IT SO YOU WILL REMEMBER IT)

- ☐ I never paste client identifying information into any tool without a signed BAA.

3

Confirm the vendor does not train on your data

A BAA covers legal responsibility, and you also want your clients' words kept out of the next model. Ask every AI vendor these four questions, and get the answers **in writing**:

- ☐ **Will you sign a BAA?**
- ☐ **Do you train your models on my data?** The answer must be no.
- ☐ **Where is data stored, and is it encrypted in transit and at rest?**
- ☐ **What runs under the hood?** Many "wrappers" quietly pass your text to a general model.

VENDOR CONFIRMED "NO TRAINING" IN WRITING ON (DATE)

Date, and who confirmed

4

Get written, specific, revocable consent

Two separate consents: **to record**, and **to use AI**. Keep it separate from your general intake form, and make clear that the client can say no at any time without it affecting their care.

The four things every client must hear about a recording:

1. What happens to it

2. Where it is stored

3. How long it is kept

4. Who has access

SAY IT LIKE THIS, COPY AND PASTE

"I record our sessions so a secure AI tool can help me draft notes. I review and finalize every note myself. It is encrypted and private, and you can say no at any time, without it affecting your care."

CHECK YOUR STATE'S RECORDING LAW

12 states require **all party** consent to record: CA, CT, DE, FL, IL, MD, MA, MT, NH, OR, PA, WA. Best practice: get it everywhere.

DOES MY STATE REQUIRE ALL PARTY CONSENT? WHAT IS MY RULE?

e.g. PA is all party, so I always get written consent

- ☐ I have written consent to record, separate from the general intake form.
- ☐ I checked my state's recording law.
- ☐ I tell every client the four things about the recording.
- ☐ I have AI use consent, and the client knows they can decline at any time.

5

No BAA? De identified text only

If you ever use a tool without a BAA, the **only** thing that may go in is text with all **18 HIPAA Safe Harbor identifiers** removed. Careful: free text notes hide identifiers, so automatic anonymization before the model sees the text is far safer than doing it by eye.

The 18 HIPAA identifiers you must strip

- Names
- Geography smaller than a state
- All dates, such as birth and admission
- Phone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate and license numbers
- Vehicle identifiers and plates
- Device identifiers and serials
- URLs
- IP addresses
- Biometric identifiers
- Full face photos and comparable images
- Any other unique identifying code

- ☐ When there is no BAA, I only ever enter de identified text, with all 18 identifiers removed.
- ☐ I rely on automatic anonymization rather than trusting my eye on free text.

6

Treat every AI output as a draft you review, edit and sign

The golden rule, from Prof. Ad de Jongh: **you stay the owner of the clinical process**. AI never makes the clinical decision, never interacts therapeutically, and never finalizes the record unchecked. You do. Every output gets your five point pass:

- ☐ **Correct** factual errors.
- ☐ **Cut** speculation the AI invented.
- ☐ **Nuance** the diagnosis with your clinical judgment.
- ☐ **Add** your own observations from the room.
- ☐ **Confirm** the final note matches what was actually said, and can be clinically defended.

7

Encrypt everything, and control who gets in

Keep ePHI encrypted **in transit and at rest**, inside systems covered by a BAA, with real access controls. Review your security every year.

- ☐ Client data is encrypted in transit and at rest.
- ☐ Access controls are in place, with strong passwords and multi factor authentication.
- ☐ Devices are locked, and I only use systems covered by a BAA for PHI.

8

Know your state's AI law and your retention period

The good news: the new state AI laws require exactly what this workbook teaches, which is that a licensed human stays responsible for anything clinical. Admin use and note taking, with consent, are explicitly fine.

IL WOPR Act, no therapeutic decisions without your review

NV AB 406

UT HB 452, disclosure

CA SB 243

NY, TX, AZ

MY STATE'S AI RULE, IN ONE LINE

e.g. IL WOPR, admin and scribing OK with consent

MY RECORD RETENTION PERIOD

Follow the longest applicable

RETENTION RULE OF THUMB

HIPAA asks 6 years for compliance **documentation**. States typically ask 5 to 10 years after last service, and for minors until majority plus the adult period. **Follow the longest that applies to you.**

- ☐ I know my state's AI law and my retention period, and I follow the longest that applies.

This is a fast moving patchwork across more than 30 states, so confirm your own state's current rules. Nothing here is legal advice.

9

Have a breach plan

If data is exposed, you must notify affected clients and HHS **within 60 days**, plus a media notice if 500 or more people are affected. Write down the plan now, while you are calm.

MY BREACH RESPONSE, WHO I CONTACT AND THE FIRST STEPS

- ☐ I have a written breach plan, and I know the 60 day notification deadline.

Write down your risk analysis, and review it yearly

A written risk analysis is a HIPAA requirement, not a nicety. Do it once, then put a yearly reminder in your calendar. One more discipline: if clients use AI themselves, keep it to **support and psychoeducation**, never positioned as the therapist.

RISK ANALYSIS COMPLETED ON

NEXT ANNUAL REVIEW DUE

mm/dd/yyyy

mm/dd/yyyy

- ☐ I have a written risk analysis, and a yearly review date in my calendar.
- ☐ Any client facing AI use stays support and psychoeducation, never AI as the therapist.

You are using AI the way it is meant to be used

All boxes ticked? Then AI drafts, and you decide and sign.

Keep the judgment, lose the paperwork.

Do all of this in one compliant workflow, book your call at <https://us.wemindtherapy.com/plans>

WeMind builds the BAA, consent, anonymization and prompts into one place, so you do not assemble compliance by hand.

Book a call and we onboard you personally.

LEGAL DISCLAIMER, LIMITATION OF LIABILITY

No advice, no relationship. This workbook is general educational information published by Moovd B.V. and its WeMind product. It is not legal advice, not compliance advice, not regulatory advice, not medical or clinical advice, and not a professional opinion. It does not create a client relationship, an advisory relationship, a fiduciary relationship or a duty of care of any kind between you and Moovd B.V., WeMind, or any of their affiliates, officers, directors, employees, advisers, contributors or licensors, together referred to as the Providers.

No warranty. This workbook is provided "as is" and "as available", without warranty or representation of any kind, whether express, implied or statutory, including any warranty of accuracy, completeness, currency, merchantability, fitness for a particular purpose, non infringement, or conformity with HIPAA, the HITECH Act, state or federal law, professional licensing rules, payer requirements or any other legal or regulatory obligation. Laws, regulations and professional guidance on artificial intelligence in healthcare change frequently, vary by jurisdiction, and may have changed since publication. Vendor plans, pricing, feature exclusions and BAA terms change without notice. No part of this workbook is guaranteed to be accurate, complete or current at the moment you read it.

No rights, no binding effect, no reliance. No right, claim, entitlement, expectation or obligation may be derived from this workbook, from its use, or from any statement contained in it. Nothing in it is binding on the Providers. Completing this workbook, in whole or in part, does not make you, your practice, your workflow, your vendors or any tool compliant with any law or standard, and it may not be presented or relied upon as evidence of compliance, certification, accreditation, approval or due diligence before any regulator, auditor, court, licensing board, insurer, payer, employer or client. Any use of this workbook is at your own discretion and entirely at your own risk.

Your sole responsibility. You are solely and exclusively responsible for your own legal and regulatory compliance, for your clinical judgment and clinical decisions, for the security and lawful processing of client information, for obtaining valid consent, for your agreements with vendors, and for verifying every point in this workbook with qualified legal counsel licensed in your own jurisdiction, and with your own professional body and insurer, before acting.

Limitation of liability. To the fullest extent permitted by applicable law, the Providers accept no liability whatsoever, whether in contract, tort including negligence, statute or otherwise, for any loss or damage of any kind, whether direct, indirect, incidental, special, consequential, punitive or exemplary, including without limitation loss of profit, loss of revenue, loss of business, loss or corruption of data, regulatory investigation, fine, penalty or enforcement action, breach notification cost, disciplinary or malpractice claim, loss of licensure, or reputational harm, arising out of or in any way connected with this workbook, its contents, any omission from it, or any use of or reliance on it, even if the Providers have been advised of the possibility of such loss. Where liability cannot lawfully be excluded, the aggregate liability of the Providers is limited to the minimum amount permitted by applicable law.

Third parties and references. References to named products, vendors, statutes, agencies, professional bodies or individuals are illustrative only. They are not endorsements, are not warranted to be accurate, and imply no affiliation, sponsorship or approval. Named trademarks remain the property of their respective

owners. The Providers are not responsible for the content, availability, terms or conduct of any third party site or service linked from this workbook.

Your entries stay on your device. Anything you type into the online version is stored in your own browser only. It is not transmitted to, collected by, or accessible to the Providers, and it is not a medical record. Do not enter client identifying information into this workbook.

Severability and governing law. If any provision of this disclaimer is held to be invalid or unenforceable, the remaining provisions stay in full force. This disclaimer is governed by the laws of the Netherlands, without prejudice to any mandatory protection available to you under the law of your own jurisdiction.

© 2026 Moovd B.V. All rights reserved. WeMind is a product of Moovd B.V., registered in the Netherlands. Reproduction or redistribution of this workbook, in whole or in part, without written permission is not permitted. The golden rule is referenced with attribution to Prof. Ad de Jongh, Ph.D., which does not imply his endorsement of this workbook or of any product.

● Presented by WeMind · The golden rule, after Prof. Ad de Jongh: AI drafts, you decide and sign.