

A 10-POINT SELF-AUDIT

Is your firm's AI use confidentiality-safe?

Your duty of confidentiality does not pause for a convenient tool. Before any AI touches client information, run it through these ten checks. Score one point for each box you can honestly tick.

- ☐ **1 We know exactly which AI tools our staff use.**
Shadow AI — staff pasting client info into free tools — is the most common and least visible risk.
- ☐ **2 No tool we use trains its models on our inputs.**
Many consumer tools reserve this right by default. For privileged material, that is disqualifying.
- ☐ **3 Client data is encrypted at rest and in transit.**
Confidential documents and credentials should never sit in plain text anywhere in the stack.
- ☐ **4 Public-facing and internal AI data are separated.**
If website chat and confidential staff research share one store, a misconfiguration can leak privilege.
- ☐ **5 Access is scoped by matter (ethics walls).**
Staff should retrieve only the matters they are assigned to — enforced by the tool, not just policy.
- ☐ **6 Our public chatbot never gives legal advice.**
A bot that “answers legal questions” can create UPL exposure. It should qualify and route only.
- ☐ **7 Every AI-generated draft is reviewed by an attorney.**
AI assists; the licensed attorney verifies law, citations, and judgment before anything goes out.
- ☐ **8 We have a written AI-use policy for staff.**
A short, clear policy prevents well-meaning mistakes far better than after-the-fact cleanup.
- ☐ **9 We can sign a BAA / meet data-residency needs.**
Some matters and clients require a Business Associate Agreement or data kept in a specific region.
- ☐ **10 Our vendor claims only protections it actually has.**
Be wary of fabricated certifications. Trust vendors who describe exactly what they implement — no more.

How did you score? **8–10:** strong posture — keep auditing as tools change. **5–7:** real gaps; prioritize separation of data and a no-train guarantee. **0–4:** pause AI use on client matters until the basics are in place.

Embido was built to tick every box above. No training on your data, encrypted and separated public/private architecture, matter-level **ethics walls**, a **UPL-safe** intake agent, attorney-review labels on every draft, and a **BAA plus data-residency** options on the Pro plan. We describe only the protections we actually implement — and we will never claim a certification we do not hold. See how at embido.com/security.

For general informational purposes only; not legal, compliance, or professional advice. This checklist is a starting point, not a substitute for your jurisdiction's rules of professional conduct or a formal security review. © 2026 Embido.