

The Private AI Workup

Your own AI, on hardware you own, inside your own walls. The one setup where the protected documents can finally go in, because nothing ever leaves the building.

Why this exists

Everything else in this toolkit carries the same warning: pre-approval letters, executed contracts, lockbox codes, and anything covered by financial, medical, or credit privacy law never go into any cloud AI tool, free or paid. Training off does not mean local. The data still travels to somebody else's servers and sits in their logs.

The private option: There is exactly one setup where that warning disappears: the model runs on hardware you own, in your own building, with no account, no provider, and no wire for the data to cross. Then you can put anything into it. Contracts. Client files. Case files. The whole database. It reads, sorts, summarizes, and drafts against all of it, and none of it ever leaves the room.

And I practice what I am describing. I installed my own personal large language model in my residence, on compute I purchased and set up myself. It runs every day. This is not a theory I read about. It is the machine I use for the work that is nobody else's business.

Who this is for

- ▶ **Agents and teams.** Transaction files, client records, and your full database, searchable and summarizable without a privacy question.
- ▶ **Brokerages.** A firm-wide private AI trained on your policies, forms, compliance rules, and market history. Every agent gets the firm's knowledge; the firm's data stays in the firm's building.
- ▶ **Attorneys and law offices.** Privileged files stay privileged. Discovery review, case summaries, and drafting against your own matter files with no third party in the chain of custody.
- ▶ **Any business with regulated data.** Medical, financial, credit, HR. If the law says the data cannot leave, the model comes to the data instead.

What the setup actually looks like

- ▶ **The hardware.** A capable desktop with a modern GPU handles a solo practice. Dedicated compact AI systems, the class of machine NVIDIA now builds for exactly this, run larger models for a team. A brokerage serving many agents runs a small server. Sizing it right is most of the game, and buying wrong is expensive in both directions.
- ▶ **The models.** Today's open-weight models are genuinely strong at reading, sorting, summarizing, and drafting. They run entirely on your machine and cost nothing per use once the hardware exists.

- ▶ **The software.** Turnkey runners make the model usable like any chat tool, and a private document index lets it answer questions from your own files: every contract, every policy, every past deal, searchable in plain English.
- ▶ **The training.** The system gets onboarded the same way this toolkit teaches: your context file, your voice, your compliance guardrails, plus your document library. It becomes an employee who has read everything your business ever produced and never leaves.

The straight talk on limits

- ▶ **Local models trail the frontier.** The biggest cloud models are smarter. The private system's jobs are reading, sorting, summarizing, and drafting from your documents, which is most of the daily work, and exactly the work you cannot send out.
- ▶ **The rule still stands.** AI drafts. You verify. You sign. A private model can still be wrong; it is just privately wrong.
- ▶ **You become the data center.** Physical security, backups, and who in the office can touch it are now your responsibility. That gets designed in on day one, not discovered later.
- ▶ **It pairs with the cloud, not against it.** The smart shape is both: cloud AI for public-facing work and hard reasoning, the private system for everything the cloud must never see.

How I run the build

1. **Audit.** What you handle, what the law says about it, what you want the machine to do, and who will use it.
2. **Spec.** The exact components or system for your size and budget. I help you order the right hardware the first time, no vendor markup games.
3. **Install.** Model, runner, private document index, and the chat interface your people will actually use, set up on site.
4. **Train.** Onboarded with your context files, your guardrails, and your document library. Tested against your real work.
5. **Handoff.** Your staff runs it. Written procedures, a maintenance plan, and I stay available as the advisor.

The first conversation is free

Fifteen minutes on Zoom. We figure out whether your practice actually needs a private system or whether a paid cloud workspace covers you, and you get the answer either way. If a private build is right, you leave with the spec. Book at BookWithHonor.com or call or text 661-400-1720.

Connor T. MacIvor · Connor with Honor · REALTOR since 1998 · CalDRE #01238257 · Sync Brokerage, Inc. DRE #02031490

SantaClaritaArtificialIntelligence.com/SRAR0820 · 661-400-1720