Client data handling

Automation work often means touching client files, tax documents, or case records. Here is exactly how Vitality Labs handles that data, written for CPA, bookkeeping, and law firms that need to document it.

The short version

- Your data stays in the systems you already own wherever practical. We build inside your accounts instead of copying data into ours.
- We get only the access the work needs, through a named login you create, and it is removed at handoff.
- No client data goes into an AI tool until we have reviewed that tool's data terms with you.
- A person on your team approves anything sent to clients.
- We use your data only for your project. We never sell it, share it, or reuse it.
- When the project ends, we delete our working copies and confirm it in writing.

Access

- You create a named account or delegated access for Vitality Labs. We never ask for your passwords or share logins.
- Multi-factor authentication is on for every account we use on your work.
- Access covers only the systems and folders the workflow needs. You get a written list and can remove any of it at any time.
- At handoff, we give up our access and confirm it in writing.

Storage and testing

- Finished workflows run in your accounts, or in cloud accounts set up in your firm's name, so you keep control after handoff.
- We build and test with sample or redacted data wherever practical.
- If we must hold a working copy, it stays in encrypted business storage with multi-factor authentication. Never personal accounts or removable drives.
- Logs your workflow creates stay in your systems, under your retention policy.

AI tools

- Before client data goes to an AI service, we review its terms with you: whether inputs train models, how long they are kept, where they are processed, and who can see them.
- We use business or API offerings whose terms say your inputs are not used for training, with the shortest retention available.
- Each step sends only the fields it needs, not whole files.
- AI drafts. Your staff approves before anything reaches a client.

Service providers

- Your project plan lists every tool in the workflow, what data it handles, and where it processes that data. Nothing is added without your approval.
- We don't hand client work to subcontractors without your written approval.
- Vitality Labs runs its own email and calendar on Google Workspace.

Retention and incidents

- Within 30 days of the project ending, or sooner if you ask, we delete our working copies of your data and confirm it in writing.
- If we learn of a suspected incident affecting your data, we tell you without undue delay, and within 72 hours.
- We help you with any notices you owe to clients, regulators, or insurers.

For CPA and tax firms

- The FTC Safeguards Rule generally treats tax and accounting firms as financial institutions, and your written information security plan (WISP) has to cover how you oversee service providers. IRS Publication 5708 has a WISP template.
- We give you what you need to list Vitality Labs as a service provider in your WISP: this description of our safeguards, the access list, and the tools in the workflow.
- Under IRC Section 7216, we use tax return information only to do the work you hired us for. We never use it for our own purposes or disclose it to anyone else.
- Your firm decides whether a workflow needs taxpayer consent under the Section 7216 rules. We document where data goes, including any processing outside the United States, which those rules treat more strictly.
- We will sign your firm's confidentiality agreement.

For law firms

- ABA Formal Opinion 512 (July 2024) asks lawyers using generative AI to understand the tools (Rule 1.1), protect client information (Rule 1.6), tell clients about AI use when it matters (Rule 1.4), supervise people and tools (Rules 5.1 and 5.3), and bill fairly (Rule 1.5).
- For each AI tool, we give you a written summary of its data terms so you can decide whether client consent is needed. The opinion calls for informed consent before client information goes into a tool that may learn from it.
- We work as a nonlawyer service provider under your supervision, keep a human review step in every workflow, and will sign your confidentiality terms.
- Virginia, DC, and Maryland have their own rules and ethics opinions. Your firm makes the final call.

What we don't claim

- Vitality Labs does not hold SOC 2, ISO 27001, or other security certifications. Many of the cloud providers your workflow runs on do, and we will point you to their reports.
- These are our practices, not legal or compliance advice. Your firm makes the final call on its own obligations.