

FirmDocs — Confidentiality & Architecture Memo

Prepared for law and accounting firms evaluating FirmDocs · Version 1.1 — July 2026 · firmdocs.ca

Purpose. This memo explains, in plain English, how FirmDocs handles a firm's documents and why it was designed the way it was. It is written so that a managing partner, a practice advisor, a firm's engagement leader, or an IT consultant can evaluate it directly. It describes the system's design and our commitments; it is not a legal opinion, and firms should satisfy themselves — we welcome that scrutiny.

What FirmDocs is

FirmDocs lets your team ask plain-English questions across a matter's or engagement's documents and receive answers with the source cited — the document and the page. If the answer is not in the documents, it says so rather than guessing. It currently works with digital documents (PDF and Word). It is in early access, and this memo will be updated as the product evolves.

The architecture, in one paragraph

FirmDocs runs on a single dedicated machine (about the size of a hardcover book) that is installed inside your office and joined to your office network. Everything — the AI model, the document index, the question answering — runs on that machine. The AI never calls out to the internet: no cloud services, no ChatGPT, no third-party processors. The unit initiates no outbound connections of any kind — no licence checks, no automatic update checks, no crash or usage reporting. If you unplug the office internet connection, FirmDocs keeps working. Your staff use it from their own computers through a web browser on your local network.

Where data lives

Data	Where it lives	Who can access it
Your original documents	Your existing systems — unchanged. FirmDocs works from copies loaded onto the unit.	Your firm
Document copies & search index	The FirmDocs unit, inside your office	Your firm
Questions asked & answers given	The FirmDocs unit, inside your office	Your firm
Any cloud service or FirmDocs server	Nothing. No document, question, or answer is transmitted outside your office.	—

What FirmDocs (the company) can and cannot see

- **We cannot see your documents, your questions, or your answers.** There is no telemetry, no analytics, and no remote "phone home" in the product.
- **Updates are never automatic.** The unit does not check in with any update server. Software updates are delivered only when the firm requests them and are applied with the firm's approval — offline, or over a

connection the firm opens for that purpose and closes afterward. This is why "the AI never calls out to the internet" and "updates with the firm's approval" are the same commitment, not two claims in tension.

- **Support is performed with the firm's knowledge and participation.** There is no standing remote access to the unit.
- **If you stop using FirmDocs, the unit is wiped in your presence.** Your original files are unaffected — they never lived only on the unit.

How this maps to a firm's confidentiality obligations

Law Society of Ontario, Rules of Professional Conduct, s. 3.3 (Confidentiality). A lawyer must hold client information in strict confidence. The commonly cited risk with AI tools is that they transmit client information to third-party servers, outside the lawyer's control and often outside Canada. FirmDocs was designed around this rule: client documents are never transmitted to any third party, never leave the firm's premises, and remain at all times in the firm's custody and control. We describe FirmDocs as designed around these obligations; whether a given tool satisfies a firm's professional obligations is a judgment for the firm and its advisors, and we are glad to support that review.

CPA Ontario Code of Professional Conduct, Rule 208 (Confidentiality). A CPA must not disclose confidential information concerning the affairs of a client, and remains responsible for that confidentiality when work is supported by software or third parties. FirmDocs creates no new disclosure: client records are processed entirely on hardware inside the firm's office, are never disclosed to us or to any service provider, and remain in the firm's custody throughout. The same qualification applies — designed around the rule, with the firm's own assessment welcomed.

PIPEDA. Under Canadian privacy law, organizations remain accountable for personal information under their control, including limits on use, disclosure, and safeguards. Because FirmDocs processes documents entirely on hardware inside the firm's office, the firm's existing custody and safeguard posture continues to apply — no new third-party data flows are created, no personal information is disclosed to us, and no data crosses a border.

Solicitor-client privilege (law firms). Privileged material is never disclosed to FirmDocs or any other party in the ordinary operation of the product; it is processed by software running on the firm's own premises, in the same way a local practice-management server would process it.

Fair questions we invite

- Ask us to demonstrate the unit working with the internet physically unplugged.
- Have your IT consultant inspect the network traffic — we welcome it.
- Ask what happens when the product cannot find an answer: it declines, and every answer it does give cites a document and page your staff can verify in one click.

Contact. Ahsan Zia, Founder — ahsan@firmdocs.ca — firmdocs.ca. Toronto, Ontario.

This memo describes the design and operation of FirmDocs as of the version date above. It is provided for information and does not constitute legal, compliance, or security advice.