

Claude Cowork for law firms: secure document and matter work for Canadian lawyers

Mike Pearlstein, CISSP, MSc Computer Science (AI)

Published May 26, 2026; Updated August 12, 2026



WHAT'S INSIDE

1. Can Ontario law firms use Claude Cowork without breaching confidentiality?
2. What does Claude Cowork actually do for a law firm?
3. How do the confidentiality and privilege guardrails work?
4. The oversight gap that matters for litigation hold and Law Society audits
5. Plan tier and a setup checklist for a law firm
6. Frequently Asked Questions



TRUSTED BY

Toronto law firms Hamilton manufacturers

Vancouver clinics GTA accounting firms Ontario non-profits

British Columbia professional services

Lawyers are asking a sharper version of the question every owner asks about Claude Cowork: can an agent that reads and writes files on a desktop touch client matters without breaching confidentiality? According to **Statistics Canada**, finance and insurance lead Canadian AI adoption at 40.4%, with professional, scientific and technical services at 32.4%. These are sector-level figures, not Cowork or firm-level adoption figures. The duty to get it right sits with the firm, not the software.

Mike Pearlstein, CISSP, MSc Computer Science (AI), founder of Fusion Computing, which has secured IT for Canadian law firms across Toronto, Hamilton, and Metro Vancouver since 2012.

Key takeaways

Book a Consultation

- A firm can use Claude Cowork on a Team or Enterprise plan with scoped access and a written policy. The confidentiality duty stays with the firm.
- Point Cowork at one matter folder, never the whole document-management system.
- Cowork keeps local-session history on the user's own computer, so the firm builds its own record of AI-assisted work. For litigation hold and Law Society supervision, you build that record yourself.
- Keep a lawyer signing off on anything client-facing or filed.

Can Ontario law firms use Claude Cowork without breaching confidentiality?

Yes, a firm can use Claude Cowork for client work on a Team or Enterprise plan, with scoped access and a written policy. The **Law Society of Ontario duty of confidentiality (Rule 3.3-1)** binds the firm, not the software, so the controls around the tool keep the firm onside. On the business plans, your content is not used to train Anthropic's models by default.

The reason matters. Confidentiality is the firm's obligation under the **Rules of Professional Conduct**, and no vendor setting removes it. What a firm controls is the scope: which files the agent can open, which plan governs the data, and who reviews the output.

Get those right and Cowork behaves like a careful junior who never leaves the building with a file. On the plan question, **Anthropic's privacy commitments** put the "not trained on by default" promise on the business

tiers, which is exactly where a firm's client work belongs.

It's the same secure-adoption logic we lay out in the pillar guide on [using Claude Cowork securely in your business](#), applied to a firm's duties, and it sits alongside our broader [IT for law firms](#) work.

What does Claude Cowork actually do for a law firm?

According to [Anthropic's Cowork documentation](#), Claude Cowork completes multi-step document work rather than answering a single question. For a firm, the practical jobs are first-pass document review, organizing a matter folder, building a chronology or index from a disclosure set, drafting correspondence and memos from source materials, and pulling key dates out of documents. Each one is a draft for a lawyer to verify, not a final work product.

Here is what each job looks like end to end: what you point Cowork at, what it does, what you get back, and the part that stays with a lawyer. We walk a firm through these before any pilot, the same way we scope any [AI services](#) engagement.

Five jobs Cowork does on a matter

1. First-pass document review

POINT IT AT

One matter folder of contracts, correspondence, and pleadings.

COWORK DOES

Reads every document, summarizes each, and flags clauses, gaps, and open issues.

YOU GET

A briefing memo with each issue tied to the document it came from.

YOU STILL OWN

2. Matter-file organization

POINT IT AT

A matter folder that has grown messy.

COWORK DOES

Renames files to your convention, sorts them by type and date, and flags duplicates.

YOU GET

A tidy folder and a list of what it moved or merged.

YOU STILL OWN

A lawyer verifies every finding before it informs advice.

You approve removals. Cowork asks before it deletes anything.

3. Disclosure and chronology synthesis

POINT IT AT

A disclosure or document-production set.

COWORK DOES

Builds a dated chronology or issue index, with every entry linked to its source file.

YOU GET

A chronology you can scan at a glance or drop into a brief.

YOU STILL OWN

A privilege check before anything goes to the other side.

4. Drafting correspondence and memos

POINT IT AT

The source materials, your notes, and a precedent or two.

COWORK DOES

Produces a first draft of a client letter, an internal memo, or a summary.

YOU GET

A draft to edit, never one to send as is.

YOU STILL OWN

A lawyer edits and signs. Nothing client-facing ships unreviewed.

5. Deadline and limitation extraction

POINT IT AT

Pleadings, orders, and contracts that carry dates.

COWORK DOES

Pulls every date and deadline into a single list.

YOU GET

A draft limitations list with the source noted beside each date.

YOU STILL OWN

Your practice-management system stays the record of truth.

Building a chronology from a disclosure set

WORKED EXAMPLE

Take a contract dispute with a disclosure set in one folder: a few hundred emails, the signed agreement, and two amendments. Point Cowork at the folder and ask for a dated chronology of the contract's life. It reads each document, pulls the date and the event, and returns a table of the date, what happened, and the file the entry came from.

What used to mean flipping through every PDF by hand comes back as a draft you can scan and correct. Then the lawyer does the part only a lawyer can: check the entries against the documents, confirm nothing privileged sits in the production set, and decide what belongs in the brief.

[See it on one of your matters →](#)

We scope a pilot on a single matter type, set the guardrails first, and show you what Cowork produces on your own files.

How do the confidentiality and privilege guardrails work?

According to Anthropic's deployment guidance, the core guardrail is least privilege: point Cowork at one matter folder, never the document-management root. Classify what is allowed in (working documents for the active matter) and what is not (privileged communications, client identifiers outside the folder). Keep a human reviewing anything client-facing. Cowork runs in an isolated environment on Anthropic's servers for remote sessions, or in an isolated virtual machine on the member's device for local sessions, and the prompts reach Anthropic, so scope is one control among several: also disable unneeded web, connector and MCP access, and require approval for consequential write actions.

The first thing I check is folder scope. When a firm points the agent at a synced document-management root, a single task can read every client's file. Scope it to the active matter and the file-exposure risk drops sharply, though prompt-injection, connector and web-access risk remain. The same scoping problem shows up when Copilot indexes a document management system, which we work through in our [NetDocuments and iManage Copilot integration guide for Canadian law firms](#).

Field note. The first thing I change is access. I've watched a paralegal point a desktop agent at an entire OneDrive that mirrored the DMS. We scoped it to one folder, and the same workflow that felt reckless became routine. The work's identical; the blast radius isn't.

The policy work is the other half. A short written rule set, the kind we cover in our guide on [what belongs in an AI acceptable use policy](#), names the approved tool, the data that may go in, and who may run it. I pair that policy with a technical review so scope survives contact with real staff.

Ask us to scope your pilot → Fusion Computing pairs the policy with the controls in a [cybersecurity](#) review so the firm has a defensible position if anyone asks.

The oversight gap that matters for litigation hold and Law Society audits

According to Anthropic, Claude Cowork stores its conversation history locally on each user's computer, and that activity is not captured by audit logs, the Compliance API, or data exports. The sharpest issue: litigation hold and Law Society supervision assume the firm can reconstruct what happened. Team and Enterprise owners can stream Cowork events to a SIEM through OpenTelemetry, but Anthropic is explicit that this does not replace audit logging for compliance. Cowork exports the full text of user prompts by default, along with tool parameters, file paths and user email addresses, so configure filtering or redaction at the collector and set SIEM access and retention before enabling export.

According to Anthropic's guidance on [using Cowork on Team and Enterprise plans](#), the local history "is not subject to Anthropic's standard data retention policies and cannot be centrally managed or exported by admins." The Enterprise [audit logs](#) that do exist capture metadata, not the content of the work.

Field note. When I demo the oversight gap to managing partners, I open the local Cowork history on the demo laptop and ask who else can see it. The answer I want them to sit with is nobody. I have yet to meet a firm whose litigation-hold procedure contemplated a transcript that lives only on one associate's machine, and that is the record an opposing party will ask about.

"I tell managing partners to treat Cowork the way they treat a new junior: give it one folder, watch its first week, and sign everything it drafts. I have not seen a firm regret those three rules. I have seen firms regret skipping them."

Mike Pearlstein, CISSP, CEO, Fusion Computing

That gap doesn't rule Cowork out. It means a firm has to design supervision in. If the pilot needs centralized monitoring, define the destination, filtering, access and retention before enabling OpenTelemetry.

If a record could be discoverable or subject to a hold, that's a decision for the lawyer, made before the work starts. The tool won't keep that record for you, so the firm's own log is the one that counts.

Plan tier and a setup checklist for a law firm

The plan tier is the first decision: per [Anthropic's plan lineup](#), only Team (\$25 USD monthly, \$20 USD annual, 2-seat minimum) and Enterprise carry the "not trained on by default" commitment a firm needs. A safe rollout: scope to one matter folder, keep "Manually approve" on for client files, write a usage policy, turn on OpenTelemetry monitoring, and keep a lawyer signing off.

Need the policy first? Use our [AI acceptable use policy template](#).

Cowork is available on Pro, Max, Team, and Enterprise plans per [Anthropic's release notes](#), but only the two business tiers fit client work. Here's the checklist Fusion Computing runs with a firm before the first real matter goes near the tool. In our practice the plan-tier fix is the first change we make.

Why Canadian firms bring this work to Fusion Computing

CISSP-led, a Microsoft Solutions Partner and a CompTIA Managed Services Trustmark holder, securing IT for Canadian SMBs across Toronto, Hamilton, and Metro Vancouver since 2012.

Get a CISSP-led review of how AI tools reach your client files →

1. **Choose Team or Enterprise.** A lawyer running client matters on a personal Pro or Max account is the first risk to fix.
2. **Scope to one matter folder.** Never the document-management root. Widen only with a reason.
3. **Default to “Manually approve.”** Cowork always asks before deleting files; keep approvals on for client work.
4. **Write an acceptable use policy.** Name the approved tool, the data that may go in, and who may run it.
5. **Turn on OpenTelemetry monitoring only after deciding what may be logged.** It gives the firm a structured visibility stream into what the agent did.
6. **Keep a lawyer signing off.** Nothing client-facing or filed ships without review.
7. **Map the terms to your duties.** Check Anthropic’s data handling against your Law Society obligations before go-live.

None of it’s exotic. The technical setup can be quick; the privacy, logging and approval work is what decides how long the pilot takes.

We set it up as part of the **managed IT** work we already do for firms, and the same pattern carries to **accounting firms**, **wealth management firms**, and **healthcare clinics** under their own regulators.

Firms doing municipal solicitor work will also want the **Claude Cowork guide for Ontario municipalities**, which covers MFIPPA and the new breach duties landing on January 1, 2027.

If you want a second set of eyes before your firm pilots Cowork, **talk to us** or read more about how we work. The review is CISSP-led at a Microsoft Solutions Partner, the same team that has secured Canadian firms since 2012.

Claude Cowork is worth adopting for the document-heavy work that fills a practice. Start with one low-risk workflow. If the controls hold and the numbers are right, expand from there.

Fusion Computing helps Canadian businesses across **Toronto and the GTA, Hamilton, and Metro Vancouver** with managed IT, cybersecurity, and Microsoft 365.

Frequently Asked Questions

Q. Is Claude Cowork confidential enough for client files?

Claude Cowork can handle client files when a firm runs it on a Team or Enterprise plan, scopes access to a single matter folder, and reviews the output. Cowork sessions run remotely by default on Anthropic's servers. Existing desktop deployments may still run locally, with code in an isolated virtual machine on the member's device. On Team and Enterprise plans, your content is not used to train Anthropic's models by default. Confidentiality stays the firm's duty under Law Society rules, so the controls around the tool are what make it safe.

Q. Does using Claude Cowork breach solicitor-client privilege?

Using Claude Cowork does not breach privilege by itself. The risk comes from careless use. Privilege depends on keeping privileged material confidential, so a firm should scope the agent to the documents it needs, keep privileged communications out of unscoped folders, and have a lawyer review anything before it leaves the firm. The tool is a drafting aid, not a store for privileged advice.

Q. What plan does a law firm need for Claude Cowork? —

A law firm should use the Team or Enterprise plan, not a personal Pro or Max account. Only the business tiers carry Anthropic's commitment not to train on your content by default, plus the owner and admin controls a firm needs. A lawyer running client matters on a personal account is the first risk to remediate in any rollout.

Q. Can opposing counsel discover Claude Cowork drafts? —

Possibly. A draft created with Claude Cowork is a document like any other, and its discoverability depends on what it is and where it lives, not on the tool. Because Cowork keeps local-session history on the user's computer and it cannot be centrally managed or exported by admins, a firm cannot assume those sessions are captured for a litigation hold without using the Compliance API. Decide what must be preserved before the work starts.

Want an AI use policy that holds up to your Law Society duties? →

Q. Is Claude Cowork allowed under Law Society rules? —

No Law Society rule names Claude Cowork, so the answer depends on how a firm uses it. The duties of confidentiality, competence, and supervision all apply. A firm that scopes access, writes a usage policy, keeps a lawyer reviewing output, and can account for what the tool did is in a defensible position. The obligation sits with the firm, not the vendor.

Q. How is Claude Cowork different from Harvey or CoCounsel?

Harvey and CoCounsel are legal-specific platforms built around legal research and workflows. Claude Cowork is a general agent that works inside your own files and apps on the desktop, using the same engine as Claude Code. For a firm, the practical differences are where the data lives, the admin and audit controls, and whether the tool is purpose-built for legal tasks or general document work.

Q. Does Claude Cowork work on Windows or only Mac?

Claude Cowork works on both macOS and Windows through the Claude desktop app, and it reached general availability on both on April 9, 2026. Cowork is available on paid plans across desktop, web and mobile. Web and mobile remote sessions are in beta and are rolling out gradually across plans, so confirm availability for your plan before launch. Some capabilities, such as computer use, arrived first as research previews, so confirm the current feature list for your platform inside the app.

Q. Who at the firm should run Claude Cowork?

Start with a small group who understand the matter and the confidentiality duty, not the whole firm at once. Cowork is an organization-wide setting that owners can switch on or off, and on Enterprise, groups and custom roles can restrict it to selected users or teams while Team remains organization-wide, so a deliberate pilot with named users is safer than a broad rollout. Pair it with training and a written policy before wider use.

Talk to Fusion

Put this guide to work

Fusion Computing helps Canadian SMBs adopt AI safely. The review work is CISSP-led at a Microsoft Solutions Partner and CompTIA Managed Services Trustmark holder, securing Canadian businesses since 2012.

- Managed IT support with a 1-hour priority response
- Cybersecurity, managed detection and response, and compliance reviews
- AI and Copilot consulting, including safe Claude Cowork pilots
- Microsoft 365 management and licensing

Book a 30-minute scoping call

fusioncomputing.ca/contact-us · 416-566-2845
Toronto · Hamilton · Metro Vancouver