FUSION COMPUTING FIELD GUIDE

Claude Cowork for dental practices: PHIPA-safe admin help for Canadian dental offices

Mike Pearlstein, CISSP, MSc AI

August 04, 2026

WHAT'S INSIDE

TRUSTED BY **Toronto law firms** **Hamilton manufacturers** **Vancouver clinics** **GTA accounting firms** **Ontario non-profits** **British Columbia professional services**

Dental office managers want to know whether Claude Cowork can clear the administrative pile without touching patient charts. According to Statistics Canada, 12.2% of Canadian businesses now use AI, double the 6.1% of a year earlier, so someone at the front desk is already trying these tools. A dental practice is a health information custodian, and that duty stays with the practice.

Mike Pearlstein, CISSP, MSc AI, founder of Fusion Computing, which has secured IT for Canadian healthcare practices across Toronto, Hamilton, and Metro Vancouver since 2012.

Key takeaways

- A dental practice can use Claude Cowork for administrative work on a Team or Enterprise plan with scoped access and a written policy.
- Keep personal health information out of the tool, de-identify it first, or run a documented PHIPA assessment. Prompts reach Anthropic.
- Scope it to an admin folder, never the practice management system or the imaging drive.
- Cowork stores its work locally, so it sits outside your audit logs. PHIPA expects a record of use you build yourself.

Plan a Safe Cowork Pilot

Can dental practices use Claude Cowork under PHIPA?

Yes, a dental practice can use Claude Cowork for administrative work on a Team or Enterprise plan, with access scoped to a folder that holds no patient identifiers and a written policy. According to Ontario's Personal Health Information Protection Act, a dentist is a health information custodian, so the duty to protect patient information stays with the practice. Patient data stays out of the tool, gets de-identified first, or goes through a documented PHIPA assessment.

QUICK SELF-CHECK

How AI-ready is your business, really?

Score your AI readiness across data, use cases, governance, people and ROI in about 2 minutes, with your ranked gaps and a 30/60/90-day plan.

Take the AI readiness assessment →

or book a free 30-min call →

Free · no email until you see your score, or talk to a senior engineer.

The duty to protect health information is the practice's, and no vendor setting removes it. The RCDSO's recordkeeping expectations sit on top of that for Ontario dentists. What the practice controls is the scope: which folders the agent opens, which plan governs the data, and whether any patient information is involved at all. On the business tiers, Anthropic's privacy commitments keep that data out of model training.

It's the same secure-adoption logic from the pillar guide on using Claude Cowork securely in your business, applied to a dental office, and it sits alongside our broader IT for healthcare practices work. The parallel guide for healthcare clinics covers the same custodian duties in a medical setting.

What does Claude Cowork safely do for a dental office?

> Claude Cowork is strongest at practice administration, not patient records. Per Anthropic's Cowork documentation, the agent works across local files and apps, so the safe jobs use no patient identifiers: drafting recall and reminder templates, writing insurance predetermination cover-letter templates, maintaining office policies and infection-control SOPs, organizing fee-guide references and billing-code lists, and building intake and consent templates. Each output is a draft a human reviews.

Here's how those administrative jobs map to the work, with the guardrail that keeps each one inside PHIPA. Fusion Computing walks practices through this before any pilot, the same way we scope any AI services

engagement.

Book a 30-minute call to scope Claude Cowork for your practice safely →

Task	What Cowork does	The guardrail
Recall and reminder templates	Drafts recall, rebooking, and no-show follow-up messages	Templates only; the merge happens in your own system
Insurance paperwork templates	Drafts predetermination cover letters and claim-note templates	No patient identifiers in the source folder
Policies and SOPs	Writes and updates office policies and infection-control procedures	Internal documents, no patient data
Fee and billing references	Organizes fee-guide references and billing-code lists	Reference data only, never a patient ledger
Intake and consent templates	Builds and refines intake and consent forms	Templates only, never completed forms

How do the PHIPA and patient-data guardrails work?

> According to Anthropic's deployment guidance, Cowork runs in an isolated virtual machine, but prompts still reach Anthropic, so the core guardrail is keeping personal health information out of the tool by default. Section 12(1) of PHIPA requires a custodian to protect health information against theft, loss, and unauthorized use or disclosure. Scope the agent to an administrative folder, de-identify anything that must be processed, and keep the practice management system and imaging off limits.

The mistake we flag most often is scope. When a practice points the agent at a patient-chart export or the imaging drive, every task touches PHI. Section 12(1) of PHIPA puts the protection duty on the custodian, and the charts sit in your practice management system for a reason. Scope Cowork to an administrative folder with no identifiers and the exposure drops to near zero.

> **Field note.** A first-person field observation: in the practice pilots I've run, the first thing I do is draw a hard line around the practice management system. I've seen a front desk want to summarize patient histories on day one. We start with recall templates and SOPs instead, prove the workflow, and only revisit PHI after a privacy officer signs off on an assessment.

The policy is the other half. A short 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 the policy with a technical review so the scope survives a busy recall week.

Fusion Computing pairs that policy work with a cybersecurity review so the practice has a defensible position.

The oversight gap for PHIPA records and RCDSO recordkeeping

> According to Anthropic, Claude Cowork stores its conversation history locally on each user's computer, outside audit logs, the Compliance API, and data exports. For a dental practice it matters: PHIPA assumes a custodian can account for how information was used, and the RCDSO's recordkeeping expectations assume records the practice can produce. Team and Enterprise owners can stream Cowork events to a SIEM through OpenTelemetry, which Anthropic notes does not replace audit logging for compliance.

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."

> **Field note.** When I walk a practice owner through the oversight gap, I open the local Cowork history on the demo machine and ask who else can see it. Nobody can. If a privacy complaint ever asks how a letter was produced, the record that answers it lives on one receptionist's laptop, and no practice's privacy binder contemplated that.

> *"Practice owners ask me whether Cowork can help with charts. I tell them to keep it away from charts entirely. The administrative work is where the hours go anyway, and the practices that hold that line get the time back without a PHIPA problem."*
>
> ***Mike Pearlstein**, CISSP, CEO, Fusion Computing*

That doesn't rule Cowork out. It means the practice designs its own record of AI-assisted work.

Fusion Computing wires the OpenTelemetry stream into the same monitoring we run for managed detection and response, so a practice sees tool calls and file access even though the transcript stays on the device. If a document could ever answer a patient or regulator question, the practice keeps that record on purpose.

Plan tier and a setup checklist for a dental practice

> The plan tier is the first decision: per Anthropic's plan lineup, only Team ($25 USD monthly, $20 USD annual, 5-seat minimum) and Enterprise carry the "not trained on by default" commitment a custodian needs. A safe rollout: scope to an admin folder with no identifiers, keep "ask before acting" on, write a usage policy, turn on OpenTelemetry monitoring, and route any PHI question through a documented PHIPA assessment first.

Cowork runs on Pro, Max, Team, and Enterprise plans per Anthropic's release notes, but only the two business tiers fit a custodian's work. Here's the checklist Fusion Computing runs with a practice before the tool goes anywhere near the office. The steps come from our 2026 clinic and practice pilots; in our practice the plan-tier fix is the first change we make.

> **Why Canadian practices 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.

1. **Choose Team or Enterprise.** A hygienist or front desk running office files on a personal account is the first risk to fix.
2. **Scope to an admin folder.** No patient identifiers, no chart exports, no imaging. Widen only after a privacy review.
3. **Default to "ask before acting."** Cowork always asks before deleting files; keep approvals on everywhere.
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.** It's the only visibility you have into what the agent did.
6. **Route PHI through an assessment.** Any use that touches patient information gets a documented PHIPA assessment and privacy-officer sign-off first.
7. **Map the terms to your duties.** Check Anthropic's data handling against PHIPA and RCDSO recordkeeping before go-live.

None of it's exotic, and most of it takes an afternoon.

Fusion Computing sets it up as part of the managed IT work we already do for healthcare practices, and the same pattern carries to accounting firms and law firms under their own regulators. The review work is CISSP-led at a Microsoft Solutions Partner, the same team that has secured Canadian practices since 2012.

Claude Cowork is worth adopting for the recall, insurance, and policy work that fills a dental office. The practices that set the plan, the scope, and the policy first are the ones that'll get the hours back without ever putting a chart at risk.

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 safe for patient records?

Keep patient records out of Claude Cowork. The safe pattern is administrative work only: templates, policies, and reference documents with no patient identifiers. A dental practice is a health information custodian under PHIPA, so any use that would touch patient information needs de-identification or a documented assessment with privacy-officer sign-off first.

Q. Can Claude Cowork connect to my practice management software?

Treat the answer as no by design. Cowork works across local files, so it could read an export, but the safe pattern keeps the practice management system and imaging entirely off limits. Charts stay in the system of record. The agent works in a scoped administrative folder that holds templates and references, never patient data.

Q. Does using Claude Cowork breach PHIPA? –

Using Claude Cowork does not breach PHIPA by itself. The risk comes from careless setup. A custodian should run it on a business plan, scope it to a folder with no patient identifiers, and route any proposed PHI use through a documented assessment. The protection duty in section 12(1) sits with the practice, not the tool.

Q. What plan does a dental practice need for Claude Cowork? –

A dental practice 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 custodian needs. A staff member running office files on a personal account is the first risk to remediate.

Q. Is patient information used to train the model? –

On Team and Enterprise plans, your content is not used to train Anthropic's models by default. The stronger answer for a dental office is that patient information should not reach the tool at all: administrative templates and references carry no identifiers, and anything that would involve PHI goes through a documented PHIPA assessment first.

Q. Can Claude Cowork help with CDCP and insurance paperwork? –

Yes, at the template level. Cowork can draft predetermination cover letters, claim-note templates, and checklists for plans including the Canadian Dental Care Plan, and it can organize fee-guide and billing-code references. Completed claims carry patient information, so they are filled and submitted through your own systems, never through the agent.

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. It is not available on the web or on mobile. 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 practice should run Claude Cowork? –

Start with the office manager and one or two admin staff who understand the custodian duty, not the whole team at once. Cowork is an organization-wide setting that owners can switch on or off, and granular per-user controls are limited, so a deliberate pilot with named users beats 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