

SUPERWISE® LEARN KIT · OCTOBER 2026

Using ChatGPT with client data.

A guide for accounting, law, real estate, and insurance firms: what to use AI for, what stays out, and the rule behind each line.

CONTENTS

What this kit covers

Start with the six decisions on page 3. Then read the section for your profession, copy the prompt pattern, and work through the checklist with whoever owns your firm's technology.

What every firm should decide first	3
Accounting and tax firms	4
Law firms	5
Real estate brokerages and agents	6
Insurance agencies	7
The safe prompt pattern	8
Firm checklist	9
Technical controls	10
Sources	11

Not legal or tax advice. This kit summarizes published rules and guidance as read in October 2026, with each source dated at the back. Rules differ by state and change. Confirm how they apply to your firm with your own counsel, your state bar or board, or your compliance lead before you rely on them.

What every firm should decide first

Your staff are already using ChatGPT and Claude. Six decisions turn that habit into a practice the firm can stand behind, and each one fits on a single line of a written policy.

1 TOOLS AND ACCOUNTS

Which AI tools, on which accounts, may staff use for client work?

Name the product and the plan. Business plans from OpenAI and Anthropic are not used to train models by default; personal plans are governed by each user's own settings, which the firm cannot see.^[1, 2]

Write down: the approved list, and that client work happens only on firm accounts.

2 DATA THAT STAYS OUT

Which client information never goes into a prompt?

Start from your profession's rule in the next four pages. Most firms land on the same core list: government ID numbers, account and card numbers, passwords, and anything a client agreement or regulator restricts.

Write down: the list, in your staff's words, with one example of each.

3 CONSENT

When does the client have to agree first?

For lawyers and tax preparers the rule can require it before client information goes into a tool. Decide where consent is recorded and who checks it.

Write down: the work that needs consent, and the form you use.

4 REVIEW

Who checks AI output before it reaches a client, a court, a regulator, or the public?

Every rule in this kit leaves responsibility with the professional. AI tools produce confident errors, including citations and figures that do not exist.

Write down: who reviews what, and that the reviewer signs off.

5 MISTAKES

What happens when someone pastes the wrong thing?

A fast, blame-free report is worth more than a perfect rule. Some disclosures start a notification clock, so the firm needs to hear about them the same day.

Write down: one contact, one channel, and what to preserve.

6 OWNER AND EVIDENCE

Who owns the policy, and how will you know it is followed?

A named owner approves tools and exceptions. Training, account settings, and a technical control that keeps a record (page 10) are how the firm shows the policy works.

Write down: the owner, the review date, and the record you keep.

Accounting and tax firms

Three rules overlap here: Section 7216 on tax return information, the AICPA confidentiality rule, and the FTC Safeguards Rule. In June 2026 the IRS added guidance aimed at AI directly.

USEFUL WITH CHATGPT AND CLAUDE	NEVER GOES IN
• Client letters explaining a notice, a deadline, or a document request, drafted from placeholders. • Research starting points on public law and IRS guidance, checked against the primary source. • Engagement checklists and internal procedures that hold no client data at all.	• Tax return information, including a client’s name, address, or identifying number, without a consent or a clear exception. • Social Security and taxpayer ID numbers, bank details, and account numbers. • Whole source documents: returns, W- 2s, 1099s, and financial statements.

THE GOVERNING RULE · IRC § 7216 AND TREAS. REG. § 301.7216

A disclosure is making tax return information known “to any person in any manner whatever.” The regulations name no AI services, and whether a given tool fits a no-consent exception is unresolved. Substantive tax analysis falls outside the preparer-to-preparer exception on its face. Consent must be written, signed, and dated before the disclosure, in the form Rev. Proc. 2013-14 sets. Penalties run to \$250 per disclosure, and a knowing or reckless disclosure is a misdemeanor.^[3, 4, 5]

Also: AICPA ET 1.700.001 bars disclosure without specific client consent, and ET 1.700.040 allows a service provider under a confidentiality contract or with consent. Tax preparers are financial institutions under the FTC Safeguards Rule, which requires oversight of service providers (§ 314.4(f)) and FTC notice within 30 days of a breach affecting 500 or more consumers. IRS OPR Issue 2026-19 (June 24, 2026) calls for secure, enterprise-approved AI only.^[6, 7, 8]

DO	DON'T
Use firm-approved business accounts, and list each AI tool in your written information security plan.	Use a personal ChatGPT or Claude account for client work.
Get a § 7216 consent before tax return information goes into a tool, or keep it out.	Treat a general privacy notice as consent.
Check every figure, citation, and code section against the source.	Send AI-drafted advice without review.
Treat an accidental paste as a possible security event and assess it the same day.	Wait to see whether anything comes of it.

Law firms

You know Rule 1.6 better than we do. What is new is the ABA's reading of it for generative AI: some tools need the client's informed consent before anything about the matter goes in.

USEFUL WITH CHATGPT AND CLAUDE	NEVER GOES IN
• First drafts of letters, routine motions, and client updates, written from a placeholder fact pattern. • Summaries of public material: a published opinion, a statute, a regulator's guidance. • Plain-English explanations of a process for a client, checked by the lawyer before sending.	• Information relating to the representation, on a tool that can learn from it, without the client's informed consent. • Privileged documents and work product pasted whole, on any account the firm does not control. • Identifiers of clients, opposing parties, and witnesses, where a placeholder does the job.

THE GOVERNING RULE · ABA FORMAL OPINION 512 (JULY 29, 2024)

For a self-learning tool, the opinion says “a client’s informed consent is required prior to inputting information relating to the representation.” General boilerplate in an engagement letter is not enough. It applies Rule 1.6(c), which requires “reasonable efforts to prevent the inadvertent or unauthorized disclosure” of client information, and it expects lawyers to read each tool’s terms of use and privacy policy.^[9, 10]

Also in the opinion: competence (1.1), communication (1.4), fees (1.5), candor (3.1, 3.3), and supervision (5.1, 5.3). State rules govern; for example, Florida Bar Ethics Opinion 24-1 (January 19, 2024) recommends informed consent.^[11]

DO	DON'T
Check whether the tool learns from inputs, and get informed consent where Opinion 512 requires it.	Rely on a general AI clause in the engagement letter as consent.
Verify every citation and quotation against the reporter or the record.	File anything an AI tool cited without reading the source. In <i>Mata v. Avianca</i> (S.D.N.Y., June 22, 2023) that cost \$5,000 in sanctions. ^[12]
Bill hourly clients for the time actually spent, including review.	Charge a client for learning a tool you will use across the practice.
Give paralegals and staff written rules, and supervise their use under Rules 5.1 and 5.3.	Leave staff to choose their own tools and accounts.

Real estate brokerages and agents

Agents use AI most for marketing copy, which is exactly where the Fair Housing Act applies. Client privacy sits in state law, and it differs from state to state.

USEFUL WITH CHATGPT AND CLAUDE

- **Listing drafts** written from the property's features, then checked against fair housing rules.
- **Market summaries** built from public sales data and your own notes, with no client named.
- **Client emails and newsletters** drafted from a placeholder template.

NEVER GOES IN

- **Financial documents:** pre-approval letters, bank statements, tax returns, and account numbers.
- **Wiring and closing details,** including escrow account numbers and transfer instructions.
- **A client's private position:** why they are selling, their top price, their timeline.

THE GOVERNING RULE · FAIR HOUSING ACT, 42 U.S.C. § 3604(C)

It is unlawful to publish any notice, statement, or advertisement about the sale or rental of a dwelling that indicates a preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin. That covers copy an AI tool wrote. HUD withdrew its 2024 guidance on digital advertising in September 2025, and its April 6, 2026 notice says actions that do not comply with the Act remain subject to enforcement.^[13, 14]

Client data: state privacy laws set their own thresholds. Virginia's applies at 100,000 consumers; Texas bars small businesses from selling sensitive data without prior consent.^[15, 16] Check your state, and your brokerage's policy.

DO	DON'T
Describe the property: rooms, finishes, lot, location facts.	Describe who the home suits, such as "perfect for a young family" or "ideal for singles."
Read every AI-written listing and ad before it is published.	Let a tool post or schedule marketing on its own.
Use placeholders for buyer and seller names, addresses, and contact details.	Paste a transaction file or closing package to get a summary.
Confirm wiring instructions by phone, through a number you already have.	Put account or wiring details in any prompt.

Insurance agencies

The NAIC’s AI bulletin is written for insurers. Agencies feel it through the carriers that appoint them, and through the state privacy and data security rules that already cover producers.

USEFUL WITH CHATGPT AND CLAUDE

- **Plain-English coverage explanations** drafted from a specimen policy form, checked by a licensed agent.
- **Renewal and follow-up emails** written from a placeholder template.
- **Summaries** of carrier bulletins and state regulator notices.

NEVER GOES IN

- **Applications and claim files** with names attached, including health and driving history.
- **Identifiers:** Social Security, driver’s license, policy, and account numbers.
- **Anything a carrier agreement restricts**, which may be stricter than state law.

THE GOVERNING RULE · NAIC MODEL BULLETIN ON AI (DECEMBER 4, 2023)

The bulletin expects each insurer to maintain a written AI program covering governance, risk controls, and oversight of third-party AI systems and data. As of August 31, 2026, 25 states and DC had adopted it. Under the Gramm-Leach-Bliley Act, state insurance regulators enforce privacy for insurers and producers.^[17, 18, 19]

Data security: the NAIC Insurance Data Security Model Law (#668, October 2017) applies to licensees, producers included, and was adopted in 28 jurisdictions as of August 2025. Licensees with fewer than ten employees are exempt from its written program requirement, but not from investigating and reporting a cybersecurity event.^[20]

DO	DON'T
Ask each carrier what it expects from agencies on AI use.	Assume a carrier’s AI program ends at the carrier’s door.
Work from specimen forms and placeholders when explaining coverage.	Paste a client’s declarations page or claim notes.
Have a licensed agent review every coverage explanation before it is sent.	Let AI output stand as advice on what a policy covers.
Add AI tools to your data security program and incident plan.	Treat an accidental paste as too small to investigate.

PATTERN

The safe prompt pattern

AI tools need the shape of a problem to help with it. They rarely need the client's identity. Write the prompt with placeholders, let the tool answer, and put the real details back yourself.

- 1 **Role and task.** Say who you are and what you need: a draft, a summary, a checklist, a plain-English explanation.
- 2 **Placeholders for identity.** Replace names, contact details, ID and account numbers, addresses, and case or policy numbers with labels such as [CLIENT] or [POLICY_N0].
- 3 **Only the facts that change the answer.** Round amounts, use ranges and roles, and leave out anything the task does not need.
- 4 **The output you want.** Length, tone, format, and audience.
- 5 **An instruction to keep the placeholders.** Ask the tool to leave every bracketed label exactly as written, so you can find and fill each one.

Worked example: a tax preparer answers an IRS notice

AS FIRST TYPED

Write an email to **Maria Delgado** (**maria.delgado@example.com**, **(615) 555-0148**) explaining the CP2000 notice she got for tax year 2024. The IRS says she left off **\$14,212** of 1099-NEC income from **Brightline Landscaping LLC**. Her SSN is **000-12-3456**. She says the income was reported on her Schedule C under her business name. Ask her to send the 1099 and her bank statements.

REWRITTEN WITH PLACEHOLDERS

I am a tax preparer. Draft a short, calm email to a client, [CLIENT], about an IRS CP2000 notice for tax year 2024. The notice says about \$14,000 of 1099-NEC income from [PAYER] was not reported. The client says it was reported on Schedule C under the client's business name, so the amounts may only need matching. Ask the client to send the Form 1099-NEC and the bank statements that show the payments. Explain that the notice has a response date and that we will prepare the reply. Keep every bracketed label exactly as written.

- **What changed.** The name, email, phone number, payer, and SSN are gone, and the amount is rounded. The tool can write the same email from what is left.
- **What still needs judgment.** Facts about a client can identify them without any name. Keep a prompt to the facts the task needs, and check the result before it is sent.
- **Where a control helps.** A gateway such as the one on page 10 can replace the email, phone, and SSN automatically. The names in this example are the part a person has to remove.

All details in the example are invented. The SSN uses the 000 prefix, which is never issued.

CHECKLIST

Firm checklist

Work through this with the person who owns your firm's technology. Every box ticked is a line you can show a client, an examiner, or an insurer who asks how the firm uses AI.

Policy

- ☐ A written AI use policy names approved tools, restricted data, review, reporting, and an owner.
- ☐ Staff have read it, and new hires read it during onboarding.
- ☐ The policy has a review date and is revisited when a tool or rule changes.

Accounts

- ☐ Client work runs only on firm-controlled business accounts.
- ☐ Training and retention settings are checked and recorded for each tool.
- ☐ Each tool's terms of use and privacy policy have been read by someone who can explain them.
- ☐ Departing staff lose access the day they leave.

Client consent

- ☐ The work that needs client consent is listed for your profession.
- ☐ Consent forms meet your profession's rule, and signed copies are kept.

Data

- ☐ Staff know the safe prompt pattern and use placeholders by default.
- ☐ Government ID, account, and card numbers never go into a prompt.
- ☐ A technical control replaces common identifiers before a prompt leaves the PC.
- ☐ Your information security program lists AI tools as service providers.

Output

- ☐ A named reviewer checks AI output before it reaches a client, a court, a regulator, or the public.
- ☐ Citations, figures, and quoted rules are verified against the original source.
- ☐ Marketing copy is checked against fair housing and advertising rules where they apply.

Incidents and records

- ☐ Staff know who to tell, and how, when client data goes into a prompt by mistake.
- ☐ The firm knows which incidents start a notification deadline.
- ☐ A record of AI use is kept for as long as your files are.

Technical controls

A policy says what the firm expects. A control applies it at the moment a prompt is sent, and keeps a record of what happened.

Three layers, in the order to put them in place

- 1 **Firm accounts.** Move client work onto business plans the firm administers, so the firm sets training and retention once for everyone.^[1, 2]
- 2 **Identifier replacement before the prompt leaves.** Software on the PC or the firm's network can swap common identifiers for placeholders on the way out, so a mistake does not depend on someone noticing it.
- 3 **A record.** A log of what was sent, what was replaced, and when gives the owner of the policy something to review and gives the firm evidence if a client asks.

One option: SUPERWISE® Sentinel

SUPERWISE Sentinel is an AI gateway that runs on the PC. Before a prompt reaches ChatGPT or Claude, it replaces emails, phone numbers, account and card numbers, government IDs, and API keys with placeholders such as <EMAIL>, so the AI can still answer. Each request is logged with what was checked and when. It runs on the machine or in the firm's own cloud, and nothing is routed through SUPERWISE.^[21]

- **Where it works.** Windows 10 and 11, installed without admin rights. A browser extension, in preview for Chrome and Edge, covers ChatGPT and Claude.
- **What it leaves to people.** Sentinel does not redact names or passwords. The placeholder habit on page 8 still applies.
- **What it costs.** Free for 30 days, then from \$10 a month per deployment.^[22]

What a control does not do. No software makes a firm compliant with any rule in this kit. Consent, review, and the judgment about what a prompt needs stay with the professional. A control makes the routine part automatic and leaves a record of it.

See how it works for a firm: superwise.ai/sentinel/for-business/

Questions to ask any control, including ours

- **Location.** Where is the prompt inspected, and does it pass through the vendor on the way?
- **Coverage.** Which identifiers does it replace, and which does it leave alone?
- **Evidence.** What does the log record, who can read it, and how long is it kept?

REFERENCE

Sources

Primary sources, read between October 6 and October 7, 2026. Rules and vendor terms change; check the current text before relying on it.

AI TOOLS AND ACCOUNTS

- 1 OpenAI, *Business data privacy, security, and compliance*. Business, Enterprise, Edu, and API data is not used for training by default. Read through search results on October 7, 2026, since the page blocks automated reading.
openai.com/business-data
- 2 Anthropic Privacy Center, *Is my data used for model training?* (updated August 18, 2026), on commercial products; and Anthropic, *Updates to consumer terms and privacy policy* (August 28, 2025), on Free, Pro, and Max plans.
privacy.claude.com/en/articles/7996868 · anthropic.com/news/updates-to-our-consumer-terms

ACCOUNTING AND TAX

- 3 26 U.S.C. § 7216 (criminal penalty) and § 6713 (\$250 per disclosure, \$10,000 a year).
law.cornell.edu/uscode/text/26/7216 · [/6713](https://law.cornell.edu/uscode/text/26/6713)
- 4 26 C.F.R. §§ 301.7216-1, -2, and -3: definitions, permitted disclosures, and consent.
law.cornell.edu/cfr/text/26/301.7216-1
- 5 Internal Revenue Service, *Rev. Proc. 2013-14* (effective January 14, 2013): consent wording and format.
irs.gov/pub/irs-drop/rp-13-14.pdf
- 6 AICPA, *Code of Professional Conduct*, ET 1.700.001 and 1.700.040 (updated through September 2026).
pub.aicpa.org/codeofconduct/ethicsresources/et-cod.pdf
- 7 Federal Trade Commission, *Safeguards Rule*, 16 C.F.R. §§ 314.2 and 314.4, breach notice effective May 13, 2024; and *FTC Safeguards Rule: What your business needs to know* (December 2024). law.cornell.edu/cfr/text/16/314.4 · ftc.gov/business-guidance
- 8 IRS Office of Professional Responsibility, *Introductory Guidelines for Responsible AI Use in Federal Tax Practice*, Issue 2026-19 (June 24, 2026). irs.gov/pub/opr-taxpros

LAW

- 9 American Bar Association, *Formal Opinion 512: Generative Artificial Intelligence Tools* (July 29, 2024). Consent, terms of use, fees, verification, and supervision. Read from an archived copy of the ABA URL.
americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf
- 10 American Bar Association, *Model Rules of Professional Conduct*, Rule 1.6, Confidentiality of Information, and Rule 1.1, Comment 8. americanbar.org/groups/professional_responsibility
- 11 The Florida Bar, *Ethics Opinion 24-1* (January 19, 2024). Recommends informed consent before confidential information goes to a third-party AI program. floridabar.org/etopinions/opinion-24-1
- 12 *Mata v. Avianca, Inc.*, No. 1:22-cv-01461 (S.D.N.Y. June 22, 2023), Opinion and Order on Sanctions. A \$5,000 penalty for filings citing opinions that did not exist. courtlistener.com, gov.uscourts.nysd.575368.54.0

REAL ESTATE

- 13 Fair Housing Act, 42 U.S.C. § 3604(c). law.cornell.edu/uscode/text/42/3604
- 14 U.S. Department of Housing and Urban Development, Notice FR-6571-N-01, *Withdrawal of guidance documents*, Federal Register Doc. 2026-06624 (April 6, 2026), following an FHEO memo of September 17, 2025. Withdraws the April 2024 digital advertising guidance; states that the Act is still enforced. federalregister.gov/d/2026-06624

- 15 Virginia Consumer Data Protection Act, Va. Code § 59.1-576 (scope and thresholds).

law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-576

- 16 Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.107 (small businesses and sensitive data), effective July 1, 2024. Read from a secondary host of the statute. texas.public.law

INSURANCE

- 17 National Association of Insurance Commissioners, *Model Bulletin: Use of Artificial Intelligence Systems by Insurers* (adopted December 4, 2023). content.naic.org/sites/default/files/cmte-h-big-data-artificial-intelligence-wg-ai-model-bulletin.pdf.pdf

- 18 NAIC, *Implementation of the NAIC Model Bulletin*, adoption map, status as of August 31, 2026. Our count of the listed jurisdictions. content.naic.org/sites/default/files/legal-adoption-map-ai-model-bulletin.pdf

- 19 Gramm-Leach-Bliley Act, 15 U.S.C. § 6805(a)(6), enforcement by state insurance authorities.

law.cornell.edu/uscode/text/15/6805

- 20 NAIC, *Insurance Data Security Model Law* (#668, October 2017), and Government Affairs brief (August 2025) listing 28 adopting jurisdictions. content.naic.org/sites/default/files/model-law-668.pdf

SUPERWISE

- 21 SUPERWISE, *SUPERWISE Sentinel* and *Sentinel for business*. Coverage, platforms, and the names and passwords limit.

superwise.ai/sentinel · superwise.ai/sentinel/for-business

- 22 SUPERWISE, *Pricing*. Plans and the 30-day trial. superwise.ai/pricing