

SUPERWISE® LEARN KIT · OCTOBER 2026

Who is liable when AI acts: a responsibility map for one workflow

Pick one real piece of client work that runs through ChatGPT or Claude. Name who approves the tool, who checks the output, who signs, what the vendor owes, and what the professional still owes, with the rule behind each line.

Responsibility follows the work, and the tool carries none of it

When a staff member uses AI on client work, the duties that already applied still apply, to the same people. The lawyer who files, the preparer who signs, and the clinician who acts own the result. The firm owns its supervision. The vendor owes what its contract and the law say it owes. California has written part of this into statute, and part 4 shows how [15].

How to use the map

- 1 Choose one workflow.** A real one, done this month: a return prepared from client documents, a motion drafted from a file, a patient letter written from a visit note.
- 2 Fill in the sheet below,** then work through the eight stages in part 2. Write a name on every owner line and say where each piece of evidence is kept.
- 3 Stop where a line stays blank.** Part 4 lists the gaps that should pause the workflow until someone fills them.

The workflow on this map

WORKFLOW

CLIENT OR MATTER TYPE	PROFESSION AND RULE SET
AI TOOL, PLAN, AND ACCOUNT	CLIENT DATA THAT GOES IN
MAPPED BY, AND DATE	NEXT REVIEW

The roles on the map

Firm owner	Approves the tool, signs the vendor contract, and owns the response when something goes wrong.
User	The person who puts client information into the tool and produces the draft.
Reviewer	A licensed professional, or a named accountable reviewer, who checks the draft against the source.
Signing professional	The lawyer, preparer, or clinician whose name goes on the filing, the return, or the decision.
Supervisor	The person with authority over the practice who sets the rules, trains staff, and checks that the rules are followed.
Vendor	The AI provider and its subprocessors, bound by their terms, any BAA or safeguards contract, and the law that applies to them.

Not legal advice. This kit summarizes published professional rules, regulator guidance, and court decisions as read in October 2026. Rules differ by state, court, and profession, and they 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 the map.

Eight stages, an owner for each, and the evidence to keep

Tick each item when it is true for this workflow. Bracketed numbers point to the sources at the end of this kit. Each grey panel gives the rule for that stage by profession; skip the professions that are not yours.

1 Approve the tool

Owner _____

Usually the firm owner, or the person the AI policy names.

WHAT MUST HAPPEN

- ☐ **Name the tool exactly:** vendor, plan, and the firm account staff will use.
- ☐ **Read the vendor's current terms** on training use, retention, subprocessors, and incident notice, and date the reading.
- ☐ **Sign the contract the data needs** before client data goes in: a BAA for patient information, safeguards terms for taxpayer data.

EVIDENCE TO KEEP

- ☐ Approval, with date and approver
Kept in _____
- ☐ Contract and terms as read, with the date
Kept in _____
- ☐ The tool on the firm's approved list
Kept in _____

LAW Understand the tool's benefits and risks, and evaluate its confidentiality risks before use [1]. Research its retention, sharing, and self-learning policies [3].

TAX Select capable service providers, require safeguards by contract, and assess them periodically [9]. Firm leaders keep documented vetting of third-party AI tools under Circular 230 § 10.36 [7].

HEALTH HHS lists a third-party AI chatbot that handles PHI on a patient portal as a business associate [12]. A cloud service that stores or processes PHI needs a BAA [13].

2 Put client data in

Owner _____

The user, working under the firm's rules.

WHAT MUST HAPPEN

- ☐ **Use the approved firm account,** never a personal one, for client work.
- ☐ **Put in only what the task needs.** Leave out identifiers the draft can do without.
- ☐ **Check consent or authority first** wherever the profession's rule requires it.

EVIDENCE TO KEEP

- ☐ Who used the tool, for which matter
Kept in _____
- ☐ The type of client data that went in
Kept in _____
- ☐ The consent on file, where one is needed
Kept in _____

LAW Informed consent comes before information about the representation goes into a self-learning tool, and boilerplate in an engagement letter does not supply it [1].

TAX Tax return information goes in only with a § 7216 consent or an exception that covers it [8]. A CPA discloses to a service provider under a confidentiality contract or with consent [10]. OPR: client data is handled "using only secure, enterprise-approved AI" [7].

HEALTH PHI goes only to a vendor with a BAA in place, and only the minimum necessary for the purpose [12, 16].

3 Produce the draft

Owner _____

The user.

WHAT MUST HAPPEN

- ☐ **Treat the output as a first draft** until a person has checked it.
- ☐ **Keep the source documents** the draft relies on, so the reviewer can check against them.
- ☐ **Note the tool and model** that produced it.

EVIDENCE TO KEEP

- ☐ Prompt and output, or where the tool keeps them
Kept in _____
- ☐ Source documents, with the date
Kept in _____

LAW Verify output to the degree the task calls for [1]. California asks lawyers to review AI output critically before relying on it [2].

TAX OPR treats AI text as an initial draft: "Practitioners cannot rely solely on AI" [7].

4 Review

Owner _____

A licensed professional, or a named reviewer accountable for the subject.

WHAT MUST HAPPEN

- ☐ **Check every fact, figure, citation, and quotation** against the original source.
- ☐ **Check the judgment.** The conclusion has to fit this client's facts.
- ☐ **Record what changed** between the draft and the approved version.

EVIDENCE TO KEEP

- ☐ Reviewer, date, and the checks done
Kept in _____
- ☐ Changes made, and the approval
Kept in _____

LAW A bankruptcy court sanctioned a lawyer and his firm \$5,500, jointly, for a brief with fabricated quotations and citations: research done with AI must be verified, "Period." [4] The Fifth Circuit imposed \$2,500 on counsel who drafted a reply brief with AI and did not check it [5].

TAX Circular 230 § 10.22 due diligence covers AI-generated facts, citations, and calculations [6, 7].

5 Send, file, or act

Owner _____

The signing or treating professional.

WHAT MUST HAPPEN

- ☐ **Make the final decision personally.** The signature stays with a person.
- ☐ **Disclose AI use** where a court order, a client agreement, or a rule requires it.
- ☐ **File the final version** with the matter, beside the review record.

EVIDENCE TO KEEP

- ☐ Final document and its approval
Kept in _____
- ☐ Disclosures made, and the filing or delivery receipt
Kept in _____

LAW The lawyer stays responsible for what is filed and for candor to the court [1]. A client-facing chatbot is labeled as AI [3]. Check the court's local rules and standing orders before filing.

TAX OPR: "final decisions must always rest with qualified professionals" [7], and the IRS reminds preparers that software leaves their judgment and responsibility in place [11]. Written advice under § 10.37 rests on reasonable assumptions, and unverified AI output can make reliance unreasonable [6, 7].

6 Supervise

Owner _____

The managing partner, practice owner, or person with principal authority.

WHAT MUST HAPPEN

- ☐ **Write down permitted uses** and train every person who uses the tool.
- ☐ **Sample the records on a schedule** and follow up each exception.
- ☐ **Correct the process** when a sample finds a problem, and record the change.

EVIDENCE TO KEEP

- ☐ Policy and training records
Kept in _____
- ☐ Sample log, exceptions, and corrections
Kept in _____

LAW Managerial lawyers establish clear AI policies and make reasonable efforts to ensure compliance [2], and supervise lawyers and nonlawyers who use AI [1]. In the \$5,500 case the firm said it prohibited unverified AI research; the court noted it did not show how the rule reached its lawyers [4].

TAX Those with principal authority keep adequate procedures in effect for everyone in the practice (§ 10.36), which OPR applies to AI policies and training [6, 7].

HEALTH The Security Rule requires workforce training and sanctions for violations [17].

7 Operate the service

Vendor _____

The AI vendor and its subprocessors, to the extent of the contract and the law that applies to them.

WHAT THE VENDOR OWES

- ☐ **The security, retention, and training - use terms** it agreed to, for the plan the firm is on.
- ☐ **Incident notice** on the terms and timing in the contract.
- ☐ **For PHI, the BAA** and the HIPAA duties a business associate carries directly.

EVIDENCE TO KEEP

- ☐ Terms as read, the subprocessor list, and any audit report the vendor provides
Kept in _____
- ☐ Incident notices and deletion confirmations
Kept in _____

LAW Read and understand the tool's terms of use and privacy policy, or consult someone who has [1].

TAX The safeguards contract with the service provider is the firm's obligation to put in place [9].

HEALTH Business associates are directly liable for compliance with certain HIPAA requirements [12].

8 Respond to harm

Owner _____

The firm owner, with the privacy or security lead, the professional, the insurer, and counsel.

WHAT MUST HAPPEN

- ☐ **Stop the exposure** and preserve the conversation, the logs, and the files.
- ☐ **Decide with counsel** which notices are owed, to whom, and by when. Tell the professional liability carrier.
- ☐ **Correct the record:** an amended filing, corrected advice, or a notice to the client.

EVIDENCE TO KEEP

- ☐ Incident timeline and preserved evidence
Kept in _____
- ☐ Decisions, who made them, and notices sent
Kept in _____

LAW Duties of communication with the client and candor to the court apply to an error found after filing [1].

TAX The FTC is notified within 30 days of discovery when unencrypted information about 500 or more consumers is acquired without authorization [9].

HEALTH An impermissible disclosure is presumed a breach unless a four-factor assessment shows a low probability of compromise. Individuals are notified within 60 days of discovery [14].

What the vendor owes, and what you still owe

A contract can move some duties onto the vendor. The professional duties stay with the people in stages 2 to 6, whatever the contract says.

DUTY	THE VENDOR'S SHARE	YOUR FIRM'S SHARE
Confidentiality	Protect data as its terms, any BAA, or any safeguards contract promise.	Decide what goes in, on which account, with whose consent [1, 8, 12].
Security	Run the service to the security terms it agreed to, and report incidents.	Choose a capable vendor, contract for safeguards, and assess it periodically [9].
Accuracy	Only what its terms promise about output.	Verify every fact, citation, and figure before it is relied on [1, 4, 7].
The decision	None.	The signing or treating professional decides and signs [1, 7].
Supervision	None over your staff.	Policies, training, and checks that they are followed [2, 6, 17].
Claims about the tool	The vendor answers for its own marketing. The FTC fined one vendor for claiming its AI could stand in for a lawyer [18].	Relying on a claim of professional ability leaves your own duties in place.
Breach response	Notice to the firm, on the contract's terms.	Assessment, notices to clients and regulators, and correction [9, 14].

The vendor terms on file for this workflow

Fill this in from the vendor's own pages and the signed contract, for the exact plan in stage 1. Re-read it each quarter: vendors change these pages without notice.

TERM	WHAT THE VENDOR'S TERMS SAY	WHERE, AND DATE READ
Is firm data used to train models?		
How long are prompts and outputs kept?		
Where is data processed and stored?		
Which subprocessors receive it?		
How fast is the firm told of an incident?		
BAA or safeguards contract signed, and the date		
Audit evidence the vendor provides		

What courts and regulators have done, and when to stop

The cases so far punish unchecked output and overstated vendor claims. Each one lands on a stage of the map.

DATE	MATTER	WHAT HAPPENED	STAGE
2023-06-22	Mata v. Avianca, S.D.N.Y.	\$5,000 penalty for filings that cited opinions that did not exist [19].	4
2025-01-17	FTC, DoNotPay final order	\$193,000, a bar on claiming the service can substitute for a professional without evidence, and notice to past subscribers [18].	1, 7
2025-07-18	In re Martin, Bankr. N.D. Ill.	\$5,500 against the lawyer and his firm jointly, plus a course on AI, for a brief with fabricated quotations. The firm's written rule against unverified AI research did not protect it [4].	4, 6
2026-01-01	California AB 316 takes effect	Civil Code § 1714.46 bars the defense that AI acted autonomously, and keeps causation, foreseeability, and comparative fault available [15].	All
2026-02-18	Fletcher v. Experian, 5th Cir.	\$2,500 against counsel who drafted most of a reply brief with AI, failed to verify it, and was not forthcoming when asked [5].	4, 8
2026-06-24	IRS OPR Issue 2026-19	Applies Circular 230 duties of diligence, competence, supervision, written advice, fees, and confidentiality to AI use [7].	1 to 6

What the record does not hold yet. The research behind this kit, checked October 6, 2026, found no final US regulator action that charges a small professional firm specifically for putting client data into a generative AI tool. Confidentiality rules, HIPAA, and the Safeguards Rule apply to that conduct today, and their enforcement needs no AI-specific rule.

Stop the workflow until these are filled in

If anyone on the map cannot answer one of these, pause the AI step for this workflow and fix the gap first.

- ☐ **The account.** Which plan and which account the work runs on, and that it is the approved one.
- ☐ **The contract.** The vendor terms, BAA, or safeguards contract that covers this data.
- ☐ **Retention.** How long the vendor keeps prompts and outputs.
- ☐ **The reviewer.** A named person who checks the draft against the source.
- ☐ **The final approver.** The professional who signs or acts.
- ☐ **The incident owner.** The person staff call the same day something goes wrong.

Evidence for stages 2 and 6, kept automatically

Stages 2 and 6 depend on evidence that a busy firm rarely writes down: what went into a prompt, and whether the rules held. A control at the point where a prompt leaves the PC can supply part of that record.

What SUPERWISE Sentinel does

As described on superwise.ai/sentinel/, read October 8, 2026 [20]:

- **Placeholders.** It replaces emails, phone numbers, account and card numbers, government IDs, and secrets such as API keys with placeholders before a prompt reaches ChatGPT or Claude, so the AI can still answer.
- **A record.** Every request is logged with what was caught, and every inspected interaction lands in an Activity Log.
- **Where it runs.** On the machine or in the firm's own cloud. Nothing is routed through SUPERWISE.
- **Platforms.** Windows 10 and 11, a browser extension in preview for Chrome and Edge, and a CLI for macOS and Linux.

What it leaves to the map

- **Coverage.** Names and street addresses are not on its published list, so the stage 2 habit of leaving out what the task does not need still applies.
- **Reach.** It sees the traffic sent through it. A personal account on a personal phone is outside it.
- **Judgment.** It does not check output and makes no firm compliant with any rule in this kit. Review, consent, and the final decision stay with stages 2, 4, and 5.

Trying it. SUPERWISE Sentinel is free for 30 days with no card, then \$10, \$25, or \$50 a month, as listed on superwise.ai/pricing/ on October 8, 2026 [20].

Sources

Primary sources, read between October 6 and October 8, 2026, except where noted. Rules and vendor terms change; check the current text before you rely on one.

LAW

- 1 American Bar Association, *Formal Opinion 512: Generative Artificial Intelligence Tools* (July 29, 2024). Competence, confidentiality and consent, communication, candor, supervision, and fees. americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf
- 2 The State Bar of California, *Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law* (November 16, 2023). Supervisory policies, confidentiality, and critical review. calbar.ca.gov/sites/default/files/portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf
- 3 The Florida Bar, *Ethics Opinion 24-1* (January 19, 2024). Vendor policies, verification, billing, and labeling a client-facing chatbot. floridabar.org/etopinions/opinion-24-1
- 4 *In re Martin*, No. 24-bk-13368 (Bankr. N.D. Ill. July 18, 2025), Memorandum Opinion imposing Rule 9011 sanctions. ilnb.uscourts.gov/sites/ilnb/files/opinions/179623_MartinRule9011SanctionsOpinionwTransmittalSheet%201.pdf
- 5 *Fletcher v. Experian Information Solutions, Inc.*, No. 25-20086 (5th Cir. February 18, 2026). ca5.uscourts.gov/opinions/pub/25/25-20086-CV0.pdf

ACCOUNTING AND TAX

- 6 US Department of the Treasury, *Circular 230*, 31 C.F.R. Part 10, §§ 10.22, 10.35, 10.36, and 10.37. irs.gov/pub/irs-pdf/pcir230.pdf
- 7 IRS Office of Professional Responsibility, *Introductory Guidelines for Responsible AI Use in Federal Tax Practice*, Issue 2026-19 (June 24, 2026). Read from the IRS e-news bulletin. content.govdelivery.com/accounts/USIRS/bulletins/41d6e70
- 8 26 U.S.C. § 7216 and 26 C.F.R. § 301.7216-3, consent to use or disclose tax return information. law.cornell.edu/uscode/text/26/7216
- 9 Federal Trade Commission, Safeguards Rule, 16 C.F.R. Part 314, including § 314.4(f) on service providers and the breach notice effective May 13, 2024; and *FTC Safeguards Rule: What Your Business Needs to Know*. ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
- 10 AICPA, *Code of Professional Conduct*, ET 1.700.001 (confidential client information) and 1.700.040 (disclosure to a service provider). pub.aicpa.org/codeofconduct
- 11 IRS, *Due Diligence Requirements for Tax Preparers* (EITC Central, updated August 19, 2026): software “cannot replace your professional judgment or responsibility under the law”. Written for refundable-credit due diligence. irs.gov/tax-professionals/eitc-central/due-diligence-requirements-for-tax-preparers

HEALTHCARE

- 12 HHS Office for Civil Rights, *Business Associates* (content last reviewed July 30, 2026). Lists an AI chatbot on a patient portal and a CPA firm with access to PHI among business associate examples. Read from a Wayback Machine capture of October 6, 2026, since hhs.gov refused automated reading. hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
- 13 HHS, *Guidance on HIPAA & Cloud Computing*. A cloud service that stores or processes PHI is a business associate. hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/
- 14 HHS, *Breach Notification Rule*. The breach presumption, the four factors, and the deadlines. hhs.gov/hipaa/for-professionals/breach-notification/

STATUTE, REGULATION, AND ENFORCEMENT

- 15 California Assembly Bill 316 (Krell), Chapter 672, Statutes of 2025, adding Civil Code § 1714.46; approved October 13, 2025, in effect January 1, 2026. Chaptered text read from a law firm's copy, since leginfo refused automated reading. leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB316
- 16 45 C.F.R. § 164.502(b), the HIPAA minimum necessary standard. ecfr.gov/current/title-45/section-164.502
- 17 HHS, *Summary of the HIPAA Security Rule*. Workforce training and sanctions. hhs.gov/hipaa/for-professionals/security/laws-regulations/
- 18 Federal Trade Commission, *In the Matter of DoNotPay*, Decision and Order (January 17, 2025). ftc.gov/legal-library/browse/cases-proceedings/donotpay
- 19 *Mata v. Avianca, Inc.*, No. 1:22-cv-01461 (S.D.N.Y. June 22, 2023), Opinion and Order on Sanctions. [courtlistener.com, gov.uscourts.nysd.575368.54.0](https://courtlistener.com/gov.uscourts.nysd.575368.54.0)

SUPERWISE

- 20 SUPERWISE, *Sentinel and Pricing*. Coverage, the record, platforms, and prices used in part 5. superwise.ai/sentinel/ · superwise.ai/pricing/