

FRIDAY, OCTOBER 9, 2026

Nine questions to ask any AI vendor before Jan. 1

California's new AI law puts attorneys on notice to scrutinize vendors' confidentiality, data access, verification and privilege protections before using generative AI for client work.

By John M. Jensen

On Sept. 30, Gov. Gavin Newsom signed Senate Bill 574. On Jan. 1, 2027, Business and Professions Code section 6068.1 becomes the first statute in the country to say, in terms, what a lawyer owes a client when generative artificial intelligence touches the client's work. The client alerts have been thorough about what the section says. This column is about the 90 days before it takes effect, and the one conversation those alerts do not script: the one with the vendor.

The duties themselves are short. An attorney shall not delegate the practice of law to generative AI. Confidential, nonpublic or personally identifying information may be entered into such a system only where access is restricted to the attorney and to people who are themselves bound by a duty of confidentiality. The attorney must personally verify what the system produces — and SB 574 amends Code of Civil Procedure section 128.7 to make the personal reading and verification of cited authority a condition of signing a paper. And the attorney must disclose the use of generative AI to the court for every document submitted.

Three of the four duties are about the attorney's own conduct and are, in the end, matters of discipline and habit. The second — restricted access — is not. It is a statement about a system most attorneys did not build, cannot inspect, and will know only through a vendor's description of it. "Access restricted to persons bound by confidentiality" is a fact about



Shutterstock

where the client's information goes after it leaves the attorney's screen: which servers, which subcontractors, which model provider, under which contract, kept for how long, used for what. The attorney who cannot answer those questions about a tool cannot say the duty is met. The vendor can answer them. The question is whether the attorney asks.

Here are the nine questions I would put to any vendor in writing, and expect answered in writing, before a tool comes near a client file.

1. Who can access the information my firm puts in? Not "it's encrypted" — who. Roles, and the circumstances in which each role sees client content.

2. Which outside companies and third-party processors handle the data as it moves to and from the model? Identify each one by name. A tool that cannot identify its processors cannot ensure that access is restricted.

3. What confidentiality obligations bind the model provider, those companies, and those processors? Ask to see the clauses. A privacy policy is a description; a contract is an obligation.

4. Is anything retained after processing — and is anything used to train a model, or to "improve your results"? Zero retention is a specific, verifiable commitment

that some model providers offer and some do not. "We don't train on your data" is not the same promise as "we keep nothing."

5. Can access be limited to the people the attorney has permitted on one matter — and can you show me, afterward, who had access to the client's data? The statute's test is restriction; the proof of restriction is a record. A tool that cannot show who read accessed a matter cannot show that only the permitted individuals did.

6. How does the tool help me verify? Section 128.7 now puts personal verification of authority on the signing attorney. A tool that shows

its sources makes that duty possible; one that produces polished text with no path back to the record makes it a daily act of faith.

7. What does the model do without an attorney in the loop, deciding? What decisions does the model make without an attorney in the loop? This is the non-delegation question in operational form. Drafting at the attorney's direction is assistance. Deciding what to claim, what to omit, what a fact is worth, is the practice of law.

8. Does it learn, or "improve," from my clients' matters — in any form, under any name? This is the question nobody is asking, and it is where the market is heading. "Learns from anonymized outcomes — how motions performed, how strategies succeeded" is now a selling point. Anonymization is not the

test for waiver of privilege or work product; disclosure to a third party for a purpose beyond the representation can be. A system that improves itself on your client's strategy has used your client's work for someone else's benefit, whatever it calls the process.

9. Who holds the written opinion that it preserves privilege, and may I rely on it? If the vendor's answer is "our terms of service," the answer is no one.

None of these questions requires technical knowledge. They require only the habit the statute now demands: treating a vendor's system as a place the client's confidences go and asking about that place the way one would ask about any other.

One more thing to read before January. SB 574 renumbers subdivision (b) of section 128.7: the four existing certifications become para-

graph (1) (A) through (D), and the new citation-verification requirement becomes paragraph (2). Subdivision (d) (1), which bars monetary sanctions against a represented party "for a violation of paragraph (2) of subdivision (b)," is reenacted unchanged. Read literally from Jan. 1, the shield that has always protected the legal-contentions certification now points at the citation rule instead. A court would very likely read it to keep its old meaning; the Legislature plainly did not intend to expose represented parties to sanctions for their lawyers' legal arguments. But it is the kind of seam a motion gets written on, and it is worth knowing it is there.

The statute does not make any tool compliant and no vendor can, nor can a vendor guarantee an attorney's compliance. It makes the attorney responsible for knowing where the client's words go. Nine questions, in

writing, is how one comes to know. Asking these nine questions in writing is how one comes to know.

John M. Jensen is a Los Angeles attorney practicing employment, administrative and business law. He is also the founder of ClearlyConcise, a legal technology company.

