

AI and Client-Data Self-Check for Tax Practices

A short self-assessment based on the IRS Office of Professional Responsibility's June 24, 2026 alert on AI in federal tax practice (OPR Alert 2026-19) and the rules it cites. Check each box you can answer "yes" to with a written document or record you could show.

1. Client data and confidentiality

IRC §§ 7216 and 6713; Circular 230 § 10.51(a)(15). The alert warns that uploading taxpayer information to unsecured or public AI systems creates disclosure risk, and expects client data to go only to secure, enterprise-approved tools.

- ☐ Staff are told in writing not to enter client names, financial data or tax documents into public, free AI tools.
- ☐ If the firm uses generative AI with client data, it is only through a business-grade product whose terms say your data is not used to train its models.
- ☐ You have checked how your tax software and other vendors handle data when their products use AI features (before or at purchase, and when features change).

2. Accuracy and review

Circular 230 §§ 10.22, 10.35, 10.37. The alert says practitioners cannot rely solely on AI; AI output is a draft that needs human review.

- ☐ A qualified person reviews AI-assisted work (citations, calculations, facts) before it goes to a client or the IRS.
- ☐ Staff are trained to check AI-generated research against primary sources (the Code, regulations, rulings).

3. Fees

Circular 230 § 10.27. The alert says billing for time not spent, or double billing for AI-assisted work, can raise a § 10.27 issue depending on the facts.

- ☐ You have looked at whether your billing reflects the time AI actually saves, and clients are not charged for work the tool did.

4. Written procedures and training

Circular 230 § 10.36; FTC Safeguards Rule; IRS Pub. 4557. The alert expects firms with principal authority to have documented AI policies, staff training and incident procedures. The written security plan itself comes from the FTC Safeguards Rule and Pub. 4557; the alert does not mention it.

- ☐ Your written information security plan (WISP) names approved and prohibited AI uses for employees and contractors.
- ☐ Staff security training is recorded and covers AI risks, including AI-assisted phishing.
- ☐ Your incident response plan covers a leak of client data through an AI tool.

Counting your checks (9 boxes)

- 7-9** Your written record is in good shape. Keep it current as tools change.
- 4-6** You have a base, but some practices aren't written down. Each unchecked box is a document to write or a record to keep.
- 0-3** Most of this is probably done informally. Writing it down is the first step.

This is a self-assessment, not legal or tax advice, and it is not a rating of your firm. Napa Logic, Inc. is a technology firm, not a law or CPA firm. The IRS alert is introductory guidance; it does not say it creates new legal requirements, and it cites existing rules.

Napa Logic, Inc. • Oregon City • brent@napalogic.com • (503) 893-8385

Book a call: <https://napalogic.com/book-a-call/>