Feel free to use as is or amend to suit your firm

The Discovery AI Defensibility Checklist

A Guide for Counsel to Avoid Rule 37 Sanctions & Privilege Waiver

This checklist should be used by **Litigation Partners** and **E-Discovery Managers** before a single document is uploaded to an LLM.

Phase 1: Environment & Tool Vetting (The "Safe Harbor" Check)

Before processing data, you must confirm the "plumbing" of the AI tool doesn't leak.

- [ ] **Zero-Retention Verification:** Does the vendor provide a written guarantee of "Zero Data Retention" (ZDR)?
    - *How:* Check the API terms. Standard ChatGPT/Claude consumer accounts retain data; Enterprise APIs typically do not.
- [ ] **Training Opt-Out:** Is there a contractual "No-Training" clause?
    - *How:* Confirm your data is **not** used to train the global model. If it is, privilege is likely waived the moment you hit "Enter."
- [ ] **SOC 2 Type II / ISO 27001:** Does the vendor hold these security certifications?
- [ ] **Jurisdictional Data Residency:** Is the data staying in a compliant region (e.g., US-based servers for US litigation)?

Phase 2: Privilege Pre-Screening (The "Gatekeeper" Step)

- [ ] **Keyword/Metadata Strip:** Before summarizing, have you run a "Privilege Filter" to remove documents tagged as *Attny-Client* or *Work Product*?
- [ ] **PII/PHI Redaction:** Are you using a local script or "Sanitizer" to scrub Social Security numbers or health info before sending text to a cloud-based LLM?
- [ ] **The "Dummy" Prompt Test:** Use a generic prompt first. Never include the client's name or the specific legal theory in the system prompt of a public tool.

Phase 3: Tactical Execution (The "Work-Product" Defense)

To protect the AI's output as **Work Product**, you must prove it was created under attorney direction.

- [ ] **Attorney-Led Prompting:** Is the prompt written or approved by an attorney?
    - *Rule:* Document the "Human-in-the-Loop." If a paralegal runs it without oversight, it’s less likely to be protected.
- [ ] **Log of "System Instructions":** Keep a secure, internal log of the prompts used.

Feel free to use as is or amend to suit your firm

    - *Why:* If the opposition moves for Rule 37 sanctions, you need to show your "Reasonable Steps" to preserve integrity.

- [ ] **The "No-Copy" Rule:** Prohibit staff from "Copy-Pasting" AI summaries directly into court filings without a 100% manual verification of facts/citations.

Phase 4: Disclosure & Protective Orders

- [ ] **Rule 26(f) Conference:** Have you discussed AI use with opposing counsel?
    - *Pro Tip:* Get an agreement that "Inadvertent disclosure via AI tool shall not constitute a subject-matter waiver."
- [ ] **Update the Protective Order:** Add a clause specifically addressing "AI-Processed Data" to ensure it falls under the existing confidentiality umbrella.
- [ ] **Clawback Agreement (FRE 502):** Ensure a robust 502(d) Order is signed by the judge. This is your "Get Out of Jail Free" card for accidental leaks.