The Seven Options Available to Attorneys to Use LLMs and Comply with Confidentiality Requirements

Introduction

- Attorneys want to use large language models (LLMs).
- Core challenge: preserve attorney–client confidentiality.
- Several paths exist, each with strengths and pitfalls.
- Goal today: outline seven options in plain language.

The Seven Options

1. Zero data retention agreements with major vendors
2. On-premises high-end workstations
3. Hosted dedicated machines
4. Managed services with confidentiality guarantees
5. Privacy by proxy or VPN
6. Legal-specific services (Midpage, Harvey)
7. Local anonymization with public LLMs

Option 1: ZDR with Major Vendors

- Use enterprise settings from OpenAI, Anthropic, Google, AWS, Azure.
- Data not stored or used to train future models.
- Enterprise contracts formalize these commitments.

Option 1: Strengths and Weaknesses

Strengths

- Access to top models
- Low operational burden
- Clear contractual framework

Weaknesses

- Trust in vendor compliance required
- Must configure settings correctly
- Some logging may still occur

Option 2: On-Premises High-End Workstations

- Buy a powerful desktop (e.g., $5,000).
- Run open-source models locally.
- Electricity and staff time add ongoing cost.

Option 2: Strengths and Weaknesses

Strengths

- Full control, nothing leaves the office
- Predictable fixed cost

Weaknesses

- Can only run smaller models
- Requires IT support
- Noise, heat, maintenance

Option 3: Hosted Dedicated Machines

- Rent entire GPU servers in data centers.
- Off-site but exclusive to you.
- Provider handles cooling and infrastructure.

Option 3: Strengths and Weaknesses

Strengths

- High performance
- No physical noise or heat
- Greater scalability than desktops

Weaknesses

- Requires technical management
- Provider logs may exist
- Idle time costly

Option 4: Managed Services

- Services like AWS Bedrock, Google Vertex, Cohere.
- Provide LLMs with confidentiality commitments.
- Integrated into enterprise compliance frameworks.

Option 4: Strengths and Weaknesses

Strengths

- Turnkey setup, little IT burden
- Strong contractual safeguards

Weaknesses

- Fewer model choices
- More expensive than raw hardware

Option 5: Privacy by Proxy or VPN

- Route traffic through VPN or proxy.
- Idea: obscure law firm identity from model provider.

Option 5: Why It Fails

- Does not stop provider from storing data.
- Shifts subpoena risk to VPN provider.
- Adds complexity without meaningful protection.
- Not sufficient for attorney–client privilege.

Option 6: Legal-Specific Services

- Tools like Midpage and Harvey.
- Built for law firms, with confidentiality promises.
- May integrate with case law and research databases.

Option 6: Strengths and Weaknesses

Strengths

- Tailored to legal practice
- Professional-responsibility optics
- Often improve legal research accuracy

Weaknesses

- High cost (Harvey), moderate (Midpage)
- May lag behind top general models in other tasks
- Two-system workflow adds friction

Option 7: Local Anonymization

- Strip identifiers before sending to public LLM.
- Replace names and details with placeholders.

Option 7: Strengths and Weaknesses

Strengths

- In theory, could use any LLM safely
- May work for low-stakes, non-client data

Weaknesses

- Hard to anonymize fully
- Risk of re-identification from context
- Requires strong local models for anonymization

Comparative Overview

- Strongest general path: ZDR with major vendors.
- Highest control: on-prem or hosted dedicated machines.
- Legal optics: Midpage/Harvey.
- Least advisable: VPN proxy, weak anonymization.

Final Thoughts

- No single perfect solution.
- Choice depends on firm size, sensitivity of matters, and budget.
- Confidentiality requires contracts, technology, and staff training.
- Understanding these seven options helps attorneys navigate responsibly.