MPL LEGAL TECH ADVISORS

The 7-Step Legal AI Compliance Framework

YOUR COMPLETE IMPLEMENTATION GUIDE TO SAFE AI USE

Why We Created This Framework

You are aware of the compliance and malpractice risks associated with legal AI. Here are some facts:

- Butler Snow, a 300-lawyer firm, recently got sanctioned for submitting 6 fake AI-generated citations. [read here]
- Stanford & Yale's 2025 study shows even "trusted" legal AI platforms hallucinate 17-33% of the time. [find study here]

Watch both videos below: one breaks down the exact compliance steps to follow, the other shows what went wrong for firms that ignored them.

Legal AI Compliance Framework

Legal AI Tool Evaluation Framework

Seeing the risks is one thing, knowing how to avoid them is another. This blueprint gives you the **exact, 7-step compliance framework** to keep your practice and clients safe and adopt AI the right way.

Book a 15min AI & Data Readiness Check

Step 1: Audit existing AI use

"Most firms are already using AI whether they realize it or not."

1.1. THE HIDDEN AI DISCOVERY WORKSHEET

∗Check all that apply to your firm:

OBVIOUS AI TOOLS:

- ☐ ChatGPT, Claude, or similar chatbots
- ☐ Legal research platforms with AI features
- ☐ Document review tools with AI sorting
- ☐ Case management software with "smart" capabilities

HIDDEN AI TOOLS:

- ☐ Microsoft Office 365 (Copilot)
- ☐ Grammarly or writing assistants
- ☐ Google Workspace (AI in Gmail/Docs)
- ☐ Vendors that quietly added "AI features"

HIGH-RISK USAGE INDICATORS:

- ☐ Associates testing AI for case research
- ☐ Staff
- ☐ using AI for client communications
- ☐ AI outputs being included in court filings
- ☐ Client data being input into public AI tools

1.2. TEAM USAGE SURVEY TEMPLATE:

**Send this to all the team members:*

1. Have you used any AI tools for work tasks in the past 6 months?
2. Which specific tools have you used?
3. What type of information did you input? (Client names, case details, legal strategies)
4. Did you know whether these tools store or learn from your inputs?
5. Have you ever used AI output in client work or court filings?

ACTION ITEMS:

- ☐ Identify all AI tools currently in use
- ☐ Flag any unauthorized use involving client matters
- ☐ Document potential confidentiality breaches
- ☐ Create approved/banned tools list

Book a 15min AI & Data Readiness Check

Step 2: Safeguard Confidentiality & Privilege

"Public AI tools store your conversations for research and model training."

2.1. THE DATA PROTECTION PROTOCOL

RED LINES (NEVER CROSS):

- No client data, case details, or privileged information in any AI tool
- No attorney work product in systems that train on inputs
- No confidential communications in unsecured platforms

The Butler Snow Reality Check: Butler Snow's sanctions came from fake citations, but the confidentiality risk is just as serious. One data breach could cost more than any sanction.

2.2. AI VENDOR SECURITY REQUIREMENTS

MINIMUM STANDARDS (NON-NEGOTIABLE):

- ☐ Written guarantee of no training on customer data
- ☐ Explicit attorney-client privilege protections
- ☐ Data deletion capabilities upon request
- ☐ SOC 2 Type II certification
- ☐ Geographic data storage restrictions

DEAL-BREAKERS:

- ☐ Vague privacy policies
- ☐ Training on customer inputs
- ☐ No privilege protection features
- ☐ Offshore data processing without consent

ACTION ITEMS

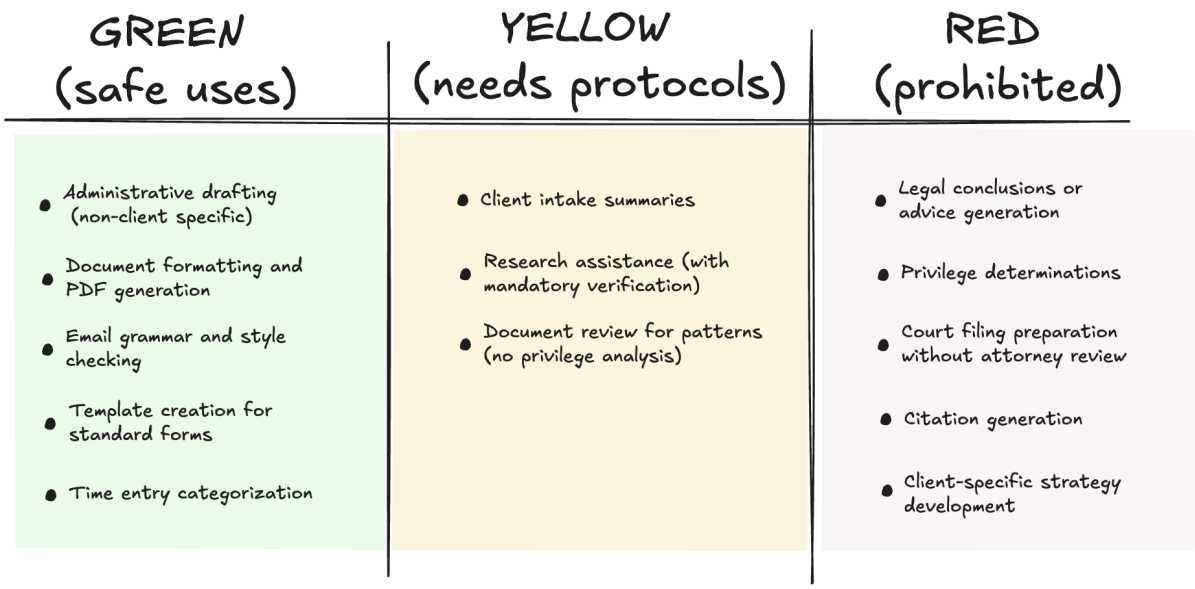
- ☐ Audit all current AI vendor agreements
- ☐ Get written data protection guarantees
- ☐ Implement input sanitization procedures
- ☐ Create privilege protection protocols

Book a 15min AI & Data Readiness Check

Step 3: Define Clear Use-Case Boundaries

"AI isn't a lawyer. It's a pattern engine, not a judgement engine."

3.1. THE TRAFFIC LIGHT SYSTEM



THE STANFORD/YALE STUDY WARNING

Even "trusted" platforms like LexisNexis (17% error rate) and Westlaw Edge (33% error rate) produce fake citations. General AI like ChatGPT has an 82% hallucination rate on legal queries.

Translation: *Never trust AI for legal citations or conclusions without verification.*

ACTION ITEMS

- ☐ Create written use-case guidelines
- ☐ Train team on traffic light system
- ☐ Implement mandatory review procedures
- ☐ Document all AI assistance in work products

Book a 15min AI & Data Readiness Check

Step 4: Build Your Firm-Wide AI Policy

"Policies aren't just insurance. They prevent unintentional errors."

4.1. THE COMPLETE AI POLICY TEMPLATE

SECTION A: APPROVED TOOLS & BANNED TOOLS

Approved tools:			
Tool name	Approved uses	Data handling verified	Renewal date

Banned tools:

- Any tool that trains on user inputs
- Any tool without explicit privilege protection
- General chatbots for legal research (82% error rate)
- [*Add specific tools based on your audit*]

SECTION B: MANDATORY PROCEDURES

Before Using AI:

1. Confirm tool is on approved list
2. Remove all client identifiers from inputs
3. Never input privileged communications
4. Save original versions before AI editing

After Using AI:

1. Attorney review required for all outputs
2. Verify all citations against primary sources
3. Fact-check all legal claims
4. Document AI assistance in work logs

SECTION C: CLIENT DISCLOSURE

Required in all engagement letters:

The following example clause, adapted from New York State Bar Association (NYSBA) reflects current best practices for AI use in legal services:

"While representing you, we may use generative AI tools and technology to assist in legal research, document drafting and other legal tasks. This technology enables us to provide more efficient and cost-effective legal services. However, it is important to note that while generative AI can enhance our work, it is not a substitute for the expertise and judgment of our attorneys. We will exercise professional judgment in using AI-generated content and ensure its accuracy and appropriateness in your specific case."

Tailor the clause to your firm:

1. Specify AI use cases
2. Inform of limitations of AI and that you assume responsibility for all legal work
3. Obtain informed client consent
4. Disclose the risks of using third-party AI software

ACTION ITEMS

- ☐ Customize policy template for your firm
- ☐ Get managing partner approval
- ☐ Distribute to all team members
- ☐ Require signed acknowledgment
- ☐ Update engagement letter templates

Book a 15min AI & Data Readiness Check

Step 5: Train Your Team on Risks & Practical Judgment

"Even the best-written policy won't matter if your team doesn't buy in."

5.1. THE BUTLER SNOW CASE STUDY TRAINING

Key learning points:

- 300-lawyer firm got sanctioned for six fake citations
- Shows even large, sophisticated firms can make costly mistakes
- Demonstrates why
- Verification is non-negotiable
- Proves that "trusted" AI tools still carry significant risk

5.2. STANFORD/YALE STUDY BRIEFING TEMPLATE

Present these facts:

- LexisNexis: 17% hallucination rate
- Westlaw Edge: 33% hallucination rate
- CoCounsel: 25% hallucination rate
- ChatGPT: 82% hallucination rate

Key Message: Even the "safe" legal AI tools produce fake citations 1 in 3 times.

5.3. PRACTICAL SCENARIO TRAINING

Scenario 1: Associate wants to use ChatGPT for case research

- **Wrong approach:** Input case facts and ask for relevant law
- **Right approach:** Use approved legal research tools with verification

Scenario 2: Team member wants to draft client email using AI

- **Wrong approach:** Include client details and case specifics
- **Right approach:** Use generic templates, remove all identifiers

Scenario 3: Partner wants to speed up brief writing with AI

- **Wrong approach:** Input brief sections with case citations
- **Right approach:** Use for formatting only, verify all citations independently

ACTION ITEMS

- ☐ Schedule monthly training sessions
- ☐ Create realistic scenario exercises
- ☐ Establish no-blame reporting culture
- ☐ Provide easy escalation procedures

Book a 15min AI & Data Readiness Check

Step 6: Document & Review System

"Compliance isn't set-and-forget. It's a living, evolving system."

6.1. THE COMPLIANCE TRACKING SYSTEM

Monthly AI Usage Report					
Tool used	Task type	Hours saved	Verification steps	Issues found	Approved

QUARTERLY RISK ASSESSMENT

- ☐ Review new AI tools entering market
- ☐ Update AI vendor security assessments
- ☐ Analyze usage patterns and risks
- ☐ Update policies based on industry changes
- ☐ Refresh team training on new scenarios

AUDIT TRAIL DOCUMENTS

For Every AI Use, Document:

- Date and time of use
- Tool used and specific task
- Input provided (with confirmation of data sanitization)
- Output received
- Verification steps completed

- Attorney review conducted
- Final approval for use

ACTION ITEMS

- ☐ Set up usage logging system
- ☐ Schedule quarterly policy reviews
- ☐ Create audit trail templates
- ☐ Assign compliance monitoring responsibility

Book a 15min AI & Data Readiness Check

Step 7: Start Small & Get Momentum Early

"Don't design a massive system. Pilot a realistic one."

7.1. THE SAFE PILOT MAP

CHOOSE YOUR FIRST USE CASE

- Client intake form processing (recommended)
- Document formatting and PDF generation
- Administrative email drafting
- Time entry categorization

PILOT REQUIREMENTS

- Must pass all 6 previous framework steps
- Single process, single attorney
- Clear success metrics
- 30-day time limit
- Built-in stop rules

TIMELINE

Week 1: Foundation

- Complete Steps 1-6 of this framework
- Select pilot use case and attorney
- Set up logging and monitoring

Week 2: Controlled pilot

- Run pilot with strict protocols
- Document all usage and outcomes
- Monitor for compliance issues

Week 3: Review & adjust

- Analyze pilot results
- Refine procedures based on learnings
- Update training materials

Week 4: Scale decision

- Decide whether to expand or stop
- Document lessons learned
- Plan next phase if successful

ACTION ITEMS

- ☐ Select single, low-risk use case
- ☐ Define success metrics
- ☐ Implement monitoring systems
- ☐ Schedule regular review checkpoints

Book a 15min AI & Data Readiness Check

Emergency Response Procedures

IF YOU DISCOVER UNVERIFIED AI CITATIONS IN FILED DOCUMENTS

Immediate Actions (0-24h)

1. Document exactly which citations are at risk
2. Verify each citation against primary sources
3. Identify any fabricated or incorrect citations
4. Notify court if corrections are required
5. Contact malpractice insurance carrier

Follow-up Actions (24-72h)

1. Review all recent filings for similar risks
2. Strengthen verification protocols
3. Retrain team on citation requirements
4. Consider independent compliance audit

IF CLIENT DATA WAS INPUT INTO UNSECURED AI

Crisis Management

1. Document what information was shared
2. Contact AI provider for data deletion
3. Assess client notification requirements
4. Review ethical obligations
5. Contact professional liability insurance
6. Implement stronger safeguards immediately

Quick Reference: The 7-Step Summary

1. **Audit existing AI use:** Find where AI is already embedded, even in unexpected tools
2. **Safeguard confidentiality:** Use only AI tools with data security and privilege protection
3. **Set clear boundaries:** Define what AI can and cannot do (AI isn't a lawyer)
4. **Build firm-wide policy:** Make expectations, tools, and procedures crystal clear
5. **Train your team:** Ensure everyone understands risks and real-world scenarios
6. **Document & review:** Keep living audit trails and update as tools evolve
7. **Start small:** Pilot one real process before scaling; slow is smooth, smooth is fast

Next Steps

You now have the full 7-step compliance framework turned into actionable checklists.

The Butler Snow sanctions and the Stanford/Yale study aren't just warnings, they're reminders that safe adoption can become your practice's competitive edge. While other firms risk malpractice, you have the roadmap to use AI responsibly and effectively.

1. Print this framework
2. Start with Step 1 (the audit) this week
3. Work through one step per week
4. Document everything
5. Don't skip steps; each one builds on the previous

Remember: The goal isn't to avoid AI. It's to use it without becoming the next cautionary tale.

This blueprint implements the 7-step legal AI compliance framework, incorporating lessons from the Butler Snow case, the Stanford/Yale Legal AI study, current compliance best practices, and extensive work with law firms & in-house teams. For guidance specific to your firm, visit [our website](mpladvisors.com).
