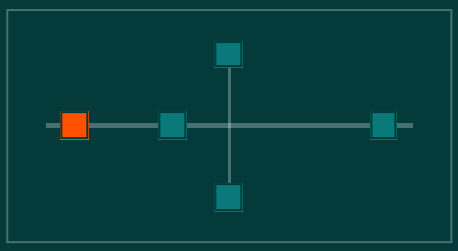
harmonic



LEGAL INDUSTRY GUIDE

The Law Firm Guide to Safe AI Adoption

> Protect client confidentiality while giving attorneys practical ways to use AI

Industry Guide | July 2026

EXECUTIVE OVERVIEW

Protect client confidentiality while giving attorneys practical ways to use AI

The CIO's job is to make approved AI use easy and prevent client information from reaching the wrong tool, account, or workflow. A written policy is necessary, but it cannot show which AI features are in use or intervene when data is about to leave the firm's control.

Before an attorney sends information to AI, five questions must have clear answers:

01	**Task:** What is the person asking AI to do?
02	**Data:** What information will the system receive?
03	**Tool:** How does the provider use, retain, and protect that information?
04	**Account:** Is the user in a firm-managed enterprise environment or a personal account?
05	**Matter:** What do the client, engagement terms, outside counsel guidelines, and applicable professional rules allow?

If an answer is unknown, pause the use and route the attorney to an approved option or an exception owner.

POLICY BASELINE

Decide what can go where

Legal information is often sensitive because of context. A matter number, draft clause, negotiation position, or witness name may not trigger a conventional data loss prevention rule, but it can still reveal client strategy or privileged work.

Adopt a firm-wide baseline, then apply stricter rules where client terms, court rules, regulation, or professional duties require them.

Permitted | Review or conditions | Stop or escalate

Data and use	Typical treatment	Minimum conditions
Public information used for brainstorming or summarization	**Generally permitted**	Firm-approved tool or account; lawyer review when the output affects legal work.
Internal firm information	**Limited**	Approved enterprise environment, business purpose, and appropriate access and retention controls.
Client confidential information	**High control**	Tool approved for the data and use case, firm-managed account, contractual safeguards, and no conflicting matter restriction.
Privileged communications or work product	**Restricted**	Specifically approved environment, practice guidance, strict access controls, and client communication or consent when required.
Regulated or highly sensitive matter data	**Restricted or prohibited**	Legal, security, and client review; additional safeguards or de-identification where appropriate.
Client information in a personal or public AI account	**Prohibited**	Block or redirect to an approved alternative.
External communication, filing, deletion, or transfer by an AI system	**Prohibited by default**	Enable only after specific approval, scoped permissions, logging, and meaningful lawyer review.

De-identification can reduce risk, but a collection of facts may still identify a client or matter.

GOVERNANCE

Establish ownership and visibility

Give one cross-functional group authority to approve tools and uses, resolve exceptions, and change controls. Include security, IT, knowledge management, risk, privacy, general counsel or ethics counsel, procurement, legal operations, and practice representatives. Name an executive sponsor and an operating owner.

The group should maintain six working deliverables:

Deliverable	Minimum content
AI inventory	Tools, embedded features, accounts, owners, users, use cases, connected systems, and review status.
Approved-use register	Approved account, permitted tasks and data, prohibited uses, owner, and next review date.
Matter restriction register	Client or matter rule, source, owner, affected teams, and review date.
Vendor assessment standard	Required security, privacy, contractual, administrative, and investigation capabilities.
Use and exception process	Short rules for common work, named approvers, response target, and recorded decisions.
Incident procedure	Reporting route, containment authority, provider contacts, evidence rules, and notification decision owners.

Inventory use across browsers, desktop applications, embedded SaaS features, plugins, APIs, local tools, and connectors. Track whether each account is enterprise-managed or personal and where users paste, upload, retrieve, or send data. Refresh the inventory as vendors add features and account settings change.

VENDOR AND USE REVIEW

Approve tools and use cases

Approve the specific account, configuration, data type, and legal task. An enterprise contract does not make every feature suitable for client information.

Review area	Answer before approval
Data use and retention	Are prompts, files, outputs, or feedback used for training or service improvement? How are active data, backups, and deletion handled?
Provider access and processing	Can personnel or subprocessors access content? Where is it processed, and how is customer data separated?
Enterprise controls	Does the service support SSO, SCIM, roles, administrator controls, audit logs, managed accounts, and configurable retention?
Feature risk	Can the feature upload files, retain memory, browse, execute code, retrieve from firm systems, or take actions? Can administrators disable or limit those functions?
Contract and incident support	Do terms protect confidentiality, limit secondary use, require incident notice, and provide useful logs and support for an investigation?
Change and exit	How are changes to models, terms, connectors, and data practices communicated? What happens to firm data when the account or contract ends?

Publish the approved-use register where attorneys already seek guidance. Reassess an approval when the provider, model, feature set, contract, retention behavior, or connected systems change. NIST's Generative AI Profile supports approved provider lists, procurement review for embedded AI, ongoing monitoring, and incident exercises.[3]

ENFORCEMENT

Put controls where data moves

Focus controls on the moment a user pastes text, uploads a file, invokes an embedded feature, or allows AI to retrieve or change information.

Surface	Minimum control set
Browser and desktop AI	Discover use, distinguish enterprise from personal accounts, inspect relevant content and destination, coach permitted alternatives, and block clear violations.
Embedded AI in SaaS	Maintain a feature inventory, review the downstream provider, configure administrator settings, and notify users when the data path changes.
Developer tools and APIs	Approve endpoints, use managed credentials, apply repository and data rules, and log relevant activity.
Connectors and agents	Use dedicated identities, least privilege, matter-scoped access where possible, action approval, audit trails, and rapid revocation.

Make controls matter-aware

- Add AI questions to client onboarding, matter intake, and outside counsel guideline review.
- Record each restriction, its source, owner, affected team, and review date.
- Make restrictions visible in the tools and workflows used by the matter team.
- Provide a route for clarification, approval, or documented client consent.

Block when the violation is clear or the likely harm is high. When context is uncertain, give a short warning that names the issue and points to an approved option or exception path.

PROFESSIONAL DUTIES

Translate duties into operating requirements

The American Bar Association applies existing duties of competence, confidentiality, communication, supervision, candor, and reasonable fees to generative AI.[1] General counsel or ethics counsel should adapt the requirements for each jurisdiction.

Duty	Operating requirement
Competence	Require initial, role- and task-specific training before lawyers and staff use approved AI tools. Cover relevant AI risks, the firm's generative AI use policy and internal protocols, approved tools and accounts, prohibited data and uses, matter restrictions, output verification, incident reporting, and exceptions. Track completion and provide refresher training when tools, risks, policies, or approved uses change.
Confidentiality and client instructions	Review data handling, apply safeguards, enforce matter restrictions, and obtain informed consent when required.
Supervision and access	Apply policy and review standards to lawyers, staff, vendors, outsourced work, and AI systems. Limit access to the information needed for the task.
Candor and review	Verify citations, quotations, authorities, factual claims, and court-facing work. A lawyer approves every filing or external legal representation.
Communication and fees	Tell clients when AI use materially affects the representation or an agreed restriction. Bill for time actually spent and explain separately charged AI costs.

Set monitoring guardrails

- Decide who can see tool names, user identities, summaries, alerts, raw prompts, files, and outputs before collection begins.
- Limit raw content access to defined investigations and audit that access.
- Set retention, masking, deletion, and legal hold rules for each data type.
- Report adoption, use cases, policy events, and unresolved exceptions to leadership without routinely exposing client content.

The audit trail should show how the firm governed AI without creating a broadly accessible second copy of sensitive legal work.

INCIDENT RESPONSE

Prepare for AI-related data incidents

Staff should report a mistaken upload or AI action immediately, without first deciding whether it qualifies as a breach.

Phase	Required action	Primary owners
Contain	Stop use, revoke a connector or token if needed, prevent further sharing, and preserve the minimum necessary evidence.	Security and IT
Establish scope	Identify the tool, account, user, data, client, matter, time, recipients, retention terms, and possible provider use or disclosure.	Security, risk, and matter counsel
Seek provider action	Request deletion or restricted processing, confirm retention behavior, preserve logs, and use contractual incident channels.	Procurement, legal, privacy, and security
Assess obligations	Decide privilege, client notice, contract, privacy, court, insurance, and regulatory obligations.	General counsel, privacy, risk, and responsible partner
Correct	Update controls, tool status, guidance, training, or matter restrictions and assign follow-up actions.	AI governance group

Do not promise deletion until the provider confirms it. Do not delay containment while debating the formal definition of the event. Counsel should decide notification and privilege issues.

Run a tabletop using a realistic scenario, such as a privileged file uploaded through a personal account or an agent retrieving documents from the wrong matter. Test the contact list, provider escalation path, decision authority, and available evidence.

AGENT CONTROLS

Set boundaries before enabling agents

Agents can retrieve data and act across document management, email, collaboration, CRM, and matter systems. California guidance says greater autonomy requires greater supervision and does not permit substantive legal decisions, legal advice, or court filings without meaningful lawyer review.[2]

Before deployment

- [ ] Start with a narrow workflow, low-sensitivity data, and a named human checkpoint.
- [ ] Use a dedicated identity, least privilege, and read-only access where possible.
- [ ] Scope credentials to the user, system, task, and matter.
- [ ] Require approval before external communication, record changes, deletion, transfers, or submissions.
- [ ] Test hidden instructions, retrieval boundaries, action limits, and access across matters.
- [ ] Log retrieval, tool calls, actions, approvals, and the responsible user. Set transaction and time limits and provide a fast way to pause the workflow and revoke access.

Reassess permissions and tests whenever the model, connector, or agent behavior changes. Expand access only after testing shows that the system stays within its assigned task and matter boundaries.

IMPLEMENTATION PLAN

A 90-day implementation plan

Use the first 90 days to establish a working baseline. The CIO or CISO should sponsor the program with general counsel, knowledge management, risk, and practice leadership.

Period	Priority	Required outputs	Evidence of completion
Days 1-30	Establish ownership and visibility	Governance group, named owners, initial inventory, account distinctions, priority use cases, and preliminary matter restrictions.	Meeting cadence, inventory, and first approved-use register.
Days 31-60	Put rules into daily work	Data and use matrix, vendor standard, role-based initial training, completion tracking, attorney examples, coaching and blocking rules, exception route, and monitoring access rules.	Published policy, configured controls, initial training completion report, documented refresher-training cadence, and tested escalation path.
Days 61-90	Connect governance to matters and response	Intake questions, restriction workflow, leadership reporting, incident tabletop, and agent baseline.	Sample matter record, completed tabletop, remediation log, and first governance report.

At each checkpoint, review actual use, attorney feedback, unresolved exceptions, and controls that repeatedly interrupt permitted work. Adjust the policy and approved options before expanding enforcement.

HARMONIC

Where Harmonic helps

Harmonic supports the controls that sit between written policy and day-to-day AI use.

Governance need	How Harmonic supports it
Discover use and distinguish destinations	Identifies activity across supported AI surfaces and separates managed enterprise use from personal or unapproved use using application and account context.
Identify sensitive legal content	Examines relevant context in supported prompts, pasted text, and files so policy can address contracts, matter information, litigation material, and other client data.
Guide or stop risky behavior	Provides coaching or enforcement at supported interaction points based on firm policy and the destination involved.
Report and investigate	Groups activity into use cases and provides role-based access, masking, retention settings, task-level summaries, and evidence for supported investigations.

The firm remains responsible for client permission and professional duties. Harmonic applies firm policies across supported AI activity. Coverage depends on the components and integrations deployed.

What to do next

1. Name the sponsor, operating owner, and exception decision makers.
2. Publish the data and use matrix and an initial approved-use register.
3. Inventory actual use, apply controls to the highest-risk data paths, and run an incident tabletop.

Selected references

1. American Bar Association, Formal Opinion 512, "Generative Artificial Intelligence Tools," July 29, 2024: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf
2. The State Bar of California, "Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law," 2026: https://www.calbar.ca.gov/sites/default/files/portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf
3. National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile," NIST AI 600-1, July 2024: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf