AI AND CLIENT CONFIDENTIALITY

# Your lawyers are already using AI. How do you protect the client file?

AI can help with research, document review and first drafts. It can also expose client information, or give confident answers that are wrong. Banning it is not enough. Lawyers need a safe way to use AI, with clear rules and a lawyer checking the result.

## THREE RISKS FOR LAW FIRMS

01

### Client information can leave the firm

Pasting a client email, contract or case history into an outside AI service sends it beyond the firm's own systems. A paid account may be secure, but that does not make it right for every client file.

02

### AI can sound certain and still be wrong

Most AI answers from memory: what it absorbed during training. When it does not know, it can invent cases, quotations and facts. The lawyer remains responsible for anything sent to a client or filed with a court.

03

### One client's file can surface in another's work

AI can search thousands of documents in seconds. Without clear access rules, information from one client's matter could appear in work for someone else.

### Where the data is stored is not the whole answer

Under the US CLOUD Act, a US technology company can sometimes be required, through valid legal process, to hand over data it controls, even when that data is held in another country. This is not routine, but it is worth understanding before client files go into any outside AI service.

## WHAT LEGAL BODIES ARE SAYING

### Protect client information, check the answer, and keep the lawyer responsible.

#### Malaysian Bar

Circular 242/2025 says members should avoid putting names, identifiers, financial information or client-specific facts into generative AI, including paid services. It calls for an internal AI policy.

#### Singapore

The Law Society and the Ministry of Law advise choosing tools that suit the confidentiality of the work, protecting privileged and personal information, and checking what the AI produces.

#### England and Wales

The Solicitors Regulation Authority warns that duties to the client and the court still apply when AI is used. Firms must protect confidential information and check the result.

**Overleaf: how Secure Law helps a firm use AI safely with confidential work.**

Sources: Malaysian Bar Circular 242/2025; Singapore Ministry of Law, Guide for Using Generative AI in the Legal Sector (2026); Law Society of Singapore advisory (2026); SRA Warning Notice on generative AI (2026). Summary only, not legal advice.

A PRACTICAL ANSWER

# Secure Law: private AI that looks things up before it answers

Secure Law, powered by SLIA (Secure Law Internet Appliance), runs in your office. It searches a private library of law and firm knowledge, then shows its sources.

INSIDE THE FIRM

THE PRIVATE LIBRARY

**Published law**
Statutes, case law and guidance where the firm practises. Kept current; new material is checked first.

**Your firm's knowledge**
Precedents, templates, approved past advice and know-how. Partners decide what goes in.

**The client's file**
Only the files for this matter, and only for the people working on it.

1. **A lawyer asks a question** →
2. **Secure Law finds the relevant passages in the library** →
3. **It drafts an answer, showing each source** →
4. **The lawyer checks and approves**

↻ **Approved work can be added to the firm's knowledge, so the library grows with every matter.**

WHY THE LIBRARY MATTERS

| | AI ANSWERING FROM MEMORY | SECURE LAW USING THE LIBRARY |
|---|---|---|
| **Source of the answer** | Training data, up to a fixed date | Current law and approved firm documents |
| **Does it know your firm?** | No. It has never seen your files | Yes. Your precedents and approved advice |
| **Can the lawyer check it?** | Sources are often unclear | Each point links to its source |
| **When it does not know** | It may fill the gap with a guess | It is designed to say so |
| **Over time** | Fixed until the provider updates it | Grows as the firm approves new work |

The technical name is retrieval-augmented generation (RAG). It reduces the risk of invented answers; a lawyer still checks.

IN SHORT

**AI is useful, but responsibility for the client's information stays with your firm.** Secure Law runs in your office, answers from sources you approve, and leaves the final decision with the lawyer. By default, client files are not sent to a public AI service.

Start with a confidential-work assessment
enquiry@intelekiq.com
intelekiq.com