



Why law firms need to prove client data is safe

The world is changing, and so are client expectations. It's no longer enough to assure clients that you protect their data — **you need to prove it.**

85%

of knowledge work organizations are already piloting, implementing, or using AI*

70%

of business leaders expect global regulations around AI and data privacy to have a transformational impact within three years*



Promises won't *cut it*

Outside Counsel Guidelines, AI mandates, audit requests. Customer demand for security proof points is rising in tandem with the growing use of AI.



AI is a *double-edged* sword

Busy lawyers can see significant benefits from adopting AI into their workflows. But without proper barriers in place, it's possible for AI to access even the most sensitive information in your DMS.

25%

of business leaders say their employees are using public AI with little oversight*

36%

of business leaders report a document policy violation due to AI tools*

65%

of business leaders rate "tools for audit trails and secure storage of sensitive information" as important*

64%

rate "customizable access rights for clients to maintain confidentiality" as important*

Manual barriers *don't scale...*

Your risk exposure is growing in our increasingly AI-reliant world. If you're still managing information barriers manually, it's going to be difficult to keep up.

...or provide *full audit trails*

Manual administration creates compliance gaps. Your audit trail is all over the place, which creates headaches when clients (and regulators) ask questions about your governance.



The consequences *are real*

Clients want proof, not promises. If you can't provide that, your clients may decide they prefer a firm that can.



40%

of clients say they would fire or consider firing a firm that experienced a breach**

66%

of clients are hesitant to work with firms that rely on outdated technology**

Can your current security model meet increasing client expectations? If the answer is no, **iManage can help.**

Security *at scale*

iManage Security Policy Manager enables organizations to protect their sensitive information by deploying information barriers at scale across client, department, or project levels.



Automation over administration

Barriers maintain themselves as matters open, timekeepers change, and laterals arrive.



Audit-ready compliance on demand

Every policy event is captured in a full timeline and can be exported in PDF or Excel instantly.



Consistent policies across channels

SPM policies pass through every iManage channel automatically, so any AI tool accessing content on a user's behalf inherits the same access controls.

* iManage Knowledge Work Benchmark Report 2026

**Integris IT, The Hidden Cost of Cyber Neglect: What Clients Really Think About Law Firms, Cybersecurity, and AI