



ARTICLE

CLOUD DOCUMENT MANAGEMENT CHANGES THE JOB FOR LEGAL TEAMS



TABLE OF CONTENTS

A CONCERN THAT RUNS DEEPER IN LEGAL WORK	4
ACCESS BECOMES SOMETHING THE FIRM MANAGES, NOT ASSUMES	4
THE JOB EXPANDS ONCE ACCESS BECOMES ROUTINE	5
ENSURING THE RECORD CAN ANSWER FOR ITSELF	6
CONNECTING THE THREADS	7



For most of the legal profession's history, keeping a client file safe didn't require much of a decision. A locked cabinet in a locked office did the job. Discovery boxes sat in a records room that nobody wandered into without a reason. A privileged memo left the building only if someone physically carried it out, and everyone in the office generally knew who had access to what simply by knowing who worked which matter. Security was less a policy than a byproduct of how a law office was built.

That approach has shifted as legal work and documentation requirements have moved onto shared drives, email, and cloud platforms. Legal teams now decide, directly and continuously, exactly who can see a file, when, and for how long. That's a very different role from the one teams once had, when a locked cabinet and a controlled office provided much of that protection by default. Contracts, discovery files, and client memos carry the same stakes that they always did. What's changed is that a team now sets and enforces those protections itself, with far more precision than a locked door ever allowed.

That shift is worth naming directly, because it changes what doing the job actually looks like day to day. A team that can say precisely who has access to a file, and remove that access the moment it's no longer warranted, is practicing law differently than a team that could only lock a door and hope. The responsibility associated with that capability doesn't belong to an IT department alone. It belongs to the people managing each matter.

A Concern That Runs Deeper in Legal Work

Based on a survey by Keypoint Intelligence®, legal organizations report a higher level of concern about document security and compliance than any other industry surveyed.¹ That concern tracks with how legal work actually functions. Privileged communications, discovery materials bound by protective orders, and client files covered by confidentiality obligations all carry consequences that go well beyond a typical data exposure. Unlike typical corporate data breaches that result in financial fines, a cloud security misconfiguration in a law firm can lead to irreversible privilege waivers, disqualified counsel, and immediate state bar disciplinary proceedings. A leaked internal memo is embarrassing, a leaked privileged communication can waive privilege entirely, and a mishandled discovery document can affect the outcome of a case.

That elevated concern reflects a fair expectation of the people managing that access, not just the tools they rely on. Being able to say who currently has access to a closed matter's discovery production, or confirm that a departed associate's account was fully removed from shared folders, provides increasingly critical operational context. Establishing these controls can support a legal team's administrative workflow and complement their efforts to represent clients responsibly.

That same concentration of sensitive material is becoming something clients notice, so it can't just be something a firm quietly manages behind the scenes. A firm that can speak clearly about who has access to a matter, and why, is offering a level of transparency that increasingly factors into how clients choose and evaluate counsel. Handled well, this becomes a genuine point of distinction instead of a burden.

Access Becomes Something the Firm Manages, Not Assumes

Deciding who can see a document is now something a legal team actively manages rather than something that a locked door managed for them by default. Access ties to the matter team itself as opposed to a department or a blanket firm-wide default. Someone working a case can see everything relevant to it without asking, and someone who has never touched the matter cannot find it by browsing around out of curiosity. That is a meaningfully different standard than paper, or early digital habits, ever actually delivered.

Access also needs to move the way legal work actually moves. A paralegal who rotates off a matter, an associate who leaves the firm, or outside counsel brought in for a single phase of litigation should lose access the moment their role on it ends. It shouldn't end because someone remembered to remove them, but because the team treats turnover as a normal part of how a matter runs. Reviewing who currently has access against who actually still needs it becomes a habit built into how the practice operates, since permissions tend to accumulate quietly over time even when people have the best intentions.

Distinguishing between viewing, editing, and approving a document gives a team a level of control that paper never really offered, since the physical act of taking a file out of a cabinet created its own rough limits. A document that only needs review doesn't need to be editable, just as a document awaiting signature shouldn't sit open to revision by everyone who can see it. Granular, matter-level permissions, set deliberately and not just inherited from a broad department folder, are what separate a team that has genuinely thought through access from one that has simply carried the same old blanket-access habit into a new format.



The Job Expands Once Access Becomes Routine

Once managing access stops requiring conscious effort, legal teams tend to turn their attention toward what leaves the firm entirely as much as what stays inside it. Legal organizations that are earlier on in their digital transformation most often point to contract review and approval as their top document opportunity, but Keypoint Intelligence® found that the most digitally advanced legal organizations among respondents surveyed ranked a different pair of priorities higher: Secure print workflows for sensitive materials and automating document redaction and discovery.¹ Contract review still matters, but for teams that have already gotten access right, it's no longer the most urgent problem.

That shift reflects where the real exposure sits once the basics are covered. A contract workflow problem is relatively contained inside the firm. A redaction or print security gap sends a document outside the firm entirely, whether through a discovery production reaching opposing counsel or a printed page left somewhere it shouldn't be. Teams that have thought this through build redaction into the export step itself, as opposed to treating it as a separate manual review that is performed at the last minute. This closes a gap that tends to open exactly when a matter is under the most time pressure.

Secure print deserves the same attention, even though it rarely comes up in the same conversation as document storage. Careful control over who can view a file can disappear the moment that file gets printed to an unmonitored device. Routing sensitive print jobs through authenticated release, where a document only prints once the requester badges in at the device, closes a gap that access control alone cannot reach.

Redaction tools can certainly be used to ensure accuracy, but they're also worth evaluating on the same basis as any other safeguard that a team relies on. A tool that permanently removes flagged text from an underlying file, instead of layering a black box over it that a determined reader can still peel away, can be the difference between redaction that works and redaction that creates a false sense of security. High-profile cases are routinely derailed when superficial 'black box' redactions are easily copied and pasted out of court filings, exposing trade secrets or confidential client identities directly to opposing counsel and the press. Confirming that distinction before a tool goes into everyday use is far less costly than discovering the gap after a document has already gone out the door.

Ensuring the Record Can Answer for Itself

Beyond just storing a document safely, staff members should be able to answer for what has happened to it. Every view, edit, download, and share tied to a document should be recorded in enough detail to answer a specific question later, not just confirm that someone opened it that day. The document must be logged using enough detail to answer a specific question at a later time. That distinction matters most in serious situations like a malpractice claim, an ethics inquiry, or a dispute over the version of a document a client actually reviewed.

That kind of record-keeping is an important risk management consideration when a firm chooses a document system. It is best integrated as a native capability rather than a post-implementation option. It is also worth confirming that records persist once a matter closes and that its files are archived, since the questions that require a clear trail often surface well after a matter is closed. A team that can only answer access questions for its currently open matters leaves half the problem unsolved.

A short, recurring review of access logs for recently closed matters catches most of the gaps before they become problems. Checking whether access was actually removed on schedule, whether any unexpected downloads occurred near the close of a matter, and whether the audit trail itself is complete for the full life of the matter takes far less time than reconstructing that same information under pressure once a dispute has already begun.





Connecting the Threads

None of this is something a legal team finishes once and sets aside. New matter types, new discovery obligations, and new client expectations will keep changing what responsible document handling looks like, often faster than any single decision anticipated.

The locked cabinet never had to account for any of that. It offered the same fixed level of protection regardless of how the matter, the client, or the firm's obligations evolved. A cloud-based practice operates under a different standard, one that has to keep pace with the work itself. The teams that treat access reviews, audit checks, and security requirements as a standing part of how they practice, rather than a project completed once and set aside, are the ones best positioned to meet that standard.

If you're ready to take the next step, connect with Canon to explore what's possible for your organization. For more information about how Canon U.S.A. can help your organization with your digital transformation goals, call 1-844-50-CANON.

¹ Source: Keypoint Intelligence, 2026 Digital Transformation Survey, U.S. Legal respondents (N=50).



1-844-50-CANON

usa.canon.com/business



The opinions expressed represent our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies. We believe that the sources of information on which our material is based are reliable and we have applied our best professional judgment to the data obtained.

This material is prepared specifically for Canon U.S.A.

Canon is a registered trademark of Canon Inc. in the United States and elsewhere. Keypoint Intelligence® is an independent authority on the document imaging industry, whose proprietary research is licensed by Canon for this article. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. Neither Canon Inc. nor Canon U.S.A., Inc. represents or warrants any third-party product or feature referenced hereunder. The authors and publishers of this content are not engaged in the rendering of professional advice or services including, without limitation, legal, or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the products and suggestions discussed in this infographic. Canon does not make any warranties concerning the accuracy or completeness of the opinions, data and other information contained in this content and, as such, assumes no liability for any errors, omissions, or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data or other information. Technical features (including automated redaction, secure printing, permissions, and audit logs) are administrative aids, not a guarantee of absolute security, and do not replace professional ethical duties. Canon does not guarantee that these features will operate error-free, prevent all unauthorized access, or run without interruption. Organizations are solely responsible for system configuration, regulatory compliance, and client confidentiality obligations.

©2026 Canon U.S.A., Inc. All rights reserved.

09/26-1581-15935