white paper:

# RIM in the age of legal discovery:

## Strategies for litigation-proofing your organization's information

Part 2: Six steps to effectively tackle legal discovery when it occurs

tab

In Part 1 of our white paper, we discussed the importance of preparing your records for the possibility of legal discovery. In this second part, we explore six steps for handling discovery when it does occur.

## Step 1. Keep RIM teams involved!

As we discussed in Part 1 of this white paper, it is important to maintain a productive working relationship between your organization's legal and RIM teams. By directly engaging RIM in the discovery process itself, the organization can draw on existing controls to locate all responsive records regardless of their age, format or location.

RIM team involvement can also ensure that in-process or pending records disposition activity is provided for any upcoming legal proceedings, preventing the destruction of records and information that may need to be preserved. This ensures that your legal counsel has the evidence it needs to pursue its case, while at the same time avoiding possible charges that it destroyed or obscured evidence in order to obstruct justice.

## Step 2. Prepare legal hold memos

Once RIM has a place at the discovery table, it can advise and support legal counsel in the drafting of a legal hold memo or equivalent document. This fundamental discovery tool advises staff across the organization that legal proceedings are pending and that potentially responsive records and information must be preserved, even if their normal retention requirements have already lapsed.

Determining exactly what constitutes "responsive records and information" is where RIM professionals come in. While it may be tempting to declare a complete moratorium on records disposition of any kind, that may not be feasible in large, multi-facetted organizations. A RIM manager can help cut through the complexity and narrow the functional scope of the legal hold to that which is truly relevant and responsive to the legal hold. Here are some key points that should be factored into the creation of a legal hold memo:

- **Which business functions are in the scope of the legal activity?** It is those same functions whose records need to be preserved for the pending legal proceedings.
- **How do materials like back-up copies, minor drafts and informal notes fit into a legal hold?** In most cases, non-record or "transitory" material are fair game for discovery. This should be confirmed up front and addressed explicitly in the legal hold memo.
- **Formats and media:** It is easy enough to say the legal hold includes records in any format or medium, but unless you spell out a wide range of examples, some key sources of evidence might be missed. Do not overlook things like email, removable drives, compact discs, maps and film media, and include them in your memo.
- **Record life cycles:** Many organizations store large collections of inactive, physical files in offsite storage centres, which can easily be overlooked and ignored. As preparation for the issuing of a legal hold, take a look at what is in storage and be sure to address it accordingly!

## Step 3. Complying with the hold: Stop and take stock

Effective RIM managers should work with legal counsel to create a recordkeeping environment that supports discovery. RIM managers can begin this process by reaching out to all areas of the company, especially those areas due to perform records disposition activity. Announce clearly and explicitly that any records disposition must be placed on hold until their records holdings are reviewed or coordinated by RIM management or legal professionals for potentially responsive material. This will allow the organization to demonstrate that it was conducted objectively and systematically.

Once responsive information has been located and preserved, disposition of non-responsive material can often resume. It is important to account for all destruction or deletion activity, including a thorough description of any materials disposed of. It is also important to apply the "when in doubt, keep it" principle so you are able to demonstrate no lingered doubts existed prior to records destruction/deletion.

## Step 4. Get a data room

While production of physical records is still very much a part of discovery, more and more efforts have been focussed on virtual data rooms, which are secure, online repositories that can be accessed remotely by authorized parties.

The creation of a virtual data room can give RIM managers unprecedented opportunity to integrate the essential techniques for organizing, retrieving and safeguarding information. Key features to include in an effective virtual data room (and RIM programs in general) are:

- access management protocols based on authorization principle
- folder hierarchies and structures based on business functions, record owners and other key filing elements
- standardized naming conventions at the container and document level
- metadata tagging and other indexing techniques
- auto-classification and full text search mechanisms
- version control and change tracking to ensure the integrity of original records
- cross-referencing of electronic document and data with physical records stored either in active working environments or inactive, offsite records centres

## Step 5. The role of document imaging

The increased use of virtual data rooms and online discovery tools can create challenges to a hybrid RIM environment. This is where document imaging can be useful. By scanning physical documents and creating an electronic copy, you can bring legacy paper into the digital realm. This allows more efficient, comprehensive access to recorded information for all parties in the discovery process.

In order to be accepted into evidence by courts, auditors and other authorities, document images need to provide assurance that they are an authentic, reliable representation of the original records. The process for scanning paper documents and electronically managing the images must be formally documented in accordance with recognized standards, such as International Standard *ISO 37.080 - Document imaging applications and National standard of Canada CAN/CGSB-72.11-93*. At a minimum, your document imaging program documentation should address the following:

- key tasks for preparing and arranging physical documents prior to scanning
- quality control procedures to ensure that each batch of images is a complete, accurate representation of the corresponding batch of paper
- standards for organizing, indexing and tagging digital copies as part of an electronic management system
- minimum technical requirements for scanning hardware, such as image resolution, flatbed size, and auto-feeder configurations

**Preserving evidence:** The disposition review is a last chance to identify records potentially responsive to litigation, investigation or audit (i.e. legal holds). In other words, it spares from destruction/deletion any records that are subject to discovery. The disposition process should include review and sign-off by multiple stakeholders, including the leadership of the department that created or captured the records, as well as representatives of the organization's legal, audit and compliance functions. For government organizations, consultations should also include those responsible for responding to requests under Freedom of Information and equivalent legislation, to ensure that any in-progress requests are also provided for.

**Avoiding "adverse inference":** Destruction of records is perfectly legal, provided that it is done in the ordinary course of business, and not a targeted attempt to hide evidence and obstruct justice. Consider the output of a disposition process: A high-level description of the records being destroyed or deleted, along with signed attestation by stakeholders who made their best efforts to identify and preserve any records needed for discovery purposes. Once discovery does happen, your organization can show that disposition was all part of a normal process, which was based on a records retention schedule built in consideration of legal requirements.

## Step 6. Be accountable

What happens when discovery-requested records have already been destroyed or deleted? It is not unusual for an organization's RIM manager to testify or give a disposition explaining the controls that were applied to ensure records were disposed of in a legally compliant manner. Remember that the goal of your records retention and disposition processes are to ensure records are kept for a reasonable amount of time, and then disposed of in a way that can be legally defended should that disposition activity ever be questioned. For the RIM professional, this means the core elements of your program can serve as direct evidence of your organization's attempt to comply with all legal requirements.

It is therefore crucial that you are ready to produce and defend the following key program components:

- **Records retention schedule:** A thoroughly documented records retention schedule can help you in two ways. First, it shows that standard records retention periods were established up front and that records were disposed of in the normal course of business. Second, if your retention schedule was developed according to the process outlined in Part 1 of this white paper, it will also provide evidence of your best attempts to comply with applicable laws. In the event that the counterparty requests records that were destroyed, you have objective proof that records were kept as long as needed to meet all reasonably identifiable requirements.

- **Disposition process:** A documented disposition program shows the review process records were subject to before they could be destroyed, deleted or transferred to an archival program. This provides evidence of "normal disposition" activity, as well as ongoing best efforts to meeting requirements that may persist after retention periods expire.

- **Disposition sign-offs and destruction certificates:** Retention schedules show when records can be destroyed, while disposition processes show how they are confirmed for destruction or deletion, where eligible. The final verification comes in for the form of signed authorizations by the business owners of records, as well as specialized stakeholders (e.g. legal counsel), stating that a specified body of records have been reviewed and are indeed eligible to be disposed of. These authorizations should also be accompanied by a destruction certificate or equivalent document attesting that the records described in the authorization were destroyed by a given method on a given date.

## What's next

Get in touch with a TAB expert today for more ways to litigation proof your records.

**UNITED STATES**
888-822-9777

**CANADA**
800.387.6212

**tab.com**