IRON MOUNTAIN®

JULY 2014

eDISCOVERY AND INFORMATION GOVERNANCE TASK FORCE REPORT

Applying Information Governance to Law Firm eDiscovery Data

LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM JULY 2014

CONTENTS

1 Background

3 Introduction

4 Stakeholder Roles in the Client ESI Governance Process

5 Implementing A New Proposed Data Intake and Tracking Process

8 The Data Intake and Tracking Process and Key IG Processes

16 Conclusion

17 References

18 Bibliography

21 Appendix A– Forms, Tools, Samples and Guidelines

31 Appendix B – Information Governance Process Wheel

BACKGROUND

The Law Firm Information Governance Symposium was established in 2012 as a platform for the legal industry to create a roadmap for information governance (IG) in the unique setting of law firms. The Symposium offers definitions, processes and best practices for building law firm IG. Firms can leverage the Symposium content to tailor an IG program that works for their culture and goals. In 2013, the Symposium Steering Committee created four task forces to work on specific, current law firm IG topics. This eDiscovery and IG Task Force report explores effectively utilizing information governance practices to manage the lifecycle of client eDiscovery data.

SYMPOSIUM STEERING COMMITTEE

BRIANNE AUL
Firmwide Records Senior Manager
Reed Smith, LLP

BRYN BOWEN, CRM
Principal
Greenheart Consulting Partners LLC

LEIGH ISAACS, CIP
Director of Records
and Information Governance
Orrick, Herrington and Sutcliffe LLP

RUDY MOLIERE
Director of Records and Information
Morgan, Lewis & Bockius LLP

CHARLENE WACENSKE
Senior Manager Firm Wide Records
Morrison & Foerster LLP

CAROLYN CASEY, ESQ.
Senior Manager, Legal Vertical
Iron Mountain

eDISCOVERY AND INFORMATION GOVERNANCE TASK FORCE

BRIAN DONATO
TASK FORCE CHAIR
Chief Information Officer
Vorys, Sater Seymour and Pease LLP

JAMES FLYNN
Director of Records & Docket
Winston & Strawn, LLP

LEIGH ISAACS, IGP, CIP, ERM
Director, Records & Information Governance
Orrick, Herrington and Sutcliffe LLP
Symposium Steering Committee Member

NORMA KNUDSON
Director of Facilities Management &
Compliance Support
Faegre Baker Daniels LLP

DANA MOORE, IGP
Manager of Records & Information
Compliance
Vedder Price PC

MICHIKO GOTO
Litigation Support Tech & Operations Manager
Winston & Strawn, LLP

BRIAN R. JENSON
Director, Litigation & eDiscovery Services
Orrick, Herrington and Sutcliffe LLP

MARK LAGODINSKI, CRM
Director of Records Management
Sidley Austin, LLP

INTRODUCTION

For many firms, a significant amount of their electronic storage is occupied by client eDiscovery data, often called electronically stored information (ESI), as defined in the amended Federal Rules of Civil Procedure (FRCP). Law firms manage vast amounts of client ESI collected in response to eDiscovery requests from opposing counsel, auditors or regulators. A typical discovery workflow may start with a drive full of client ESI, which is then processed, sorted, searched, culled, analyzed, reviewed, and eventually produced to the requesting party. Through each of these stages, the client ESI is often copied and stored in different systems inside and outside the firm. While many firms have some IG procedures in place, most have not systematically applied IG to the management of client ESI. This report explores the application of several core IG processes to the management of client ESI. It is important to call out that this report explicitly excludes dealing with the challenges that firms face when handling ESI in the firm's custody in response to a discovery request to which the firm is a party. While many of the same principles apply, a detailed treatment of the nuances is beyond the scope of this paper.

WHY SHOULD LITIGATION SUPPORT PROFESSIONALS CARE?

Client ESI is largely handled by a firm's designated litigation support resources, who are concerned with the risk management and storage of these ever-growing volumes. In addition, litigation support teams frequently handle the brunt of firm IG processes without the benefit of a documented approach for client ESI. These teams are often looking for direction on: (a) how to manage the many copies of ESI they take in, (b) what they can destroy and what they must retain (and for how long), (c) how the client ESI is secured and (d) what IG roles each employee takes on. In such an ESI approach, firms will want to be aware of any client requirements that differ from the firm's standard IG processes.

WHY SHOULD IT AND INFORMATION GOVERNANCE PROFESSIONALS CARE?

There are good reasons why client ESI should be handled differently than firm work product or administrative data. Client ESI is often voluminous, requiring large amounts of indirect cost including storage space, backups and data processing requirements, as well as vendor processing and hosting charges. These professionals also care about IG for ESI because they must ensure the firm has the security and vendor management processes to manage professional and regulatory risks.

This report outlines proposed roles, responsibilities, processes, and practical advice for using the information governance framework and key processes from the symposium reports, when implementing an information governance program to manage the lifecycle of client ESI. We have used the 2013 Symposium report, "Building Law Firm Information Governance: Prime Your Key Processes,"[1] particularly relying on the IG Framework and key processes discussions to inform our recommendations. While effectively governing ESI requires a different approach than governing firm information and work product, it is critical to draw from IG standards in several of the key processes in the framework.

WHAT ARE ESI AND eDISCOVERY?

Because many of the terms used in this report may be unfamiliar "terms of art", we will start with some basic definitions. You can find more definitions in the documents referenced in Appendix C. ESI, which stands for electronically stored information, under the FRCP, is information created, manipulated, communicated, stored, and utilized in an electronic format that requires the use of computer hardware and software to access and use.

Practically, inside law firms ESI refers to electronic information in its native format, provided by the client as part of a litigation or investigation process. Client ESI is usually loaded into different technology platforms to facilitate eDiscovery processing, analysis, review, and production. The data is culled, augmented, and copied as it moves through the eDiscovery lifecycle.

STAKEHOLDER ROLES IN CLIENT ESI GOVERNANCE

IG success requires that all stakeholders are engaged and know their roles while still understanding the processes beyond their area of responsibility. Often, there will be differing perspectives that must be resolved as part of the larger IG process. For example, a firm's records policy and retention schedule may require them to keep a document for a specific period of time, but information technology (IT) personnel may want to destroy data as quickly as possible to free up storage resources. Failure to define roles, responsibilities, and standardize processes may expose the firm to undue risks, inefficiencies, unnecessary expense, and potentially reputational damage. Each firm should consider developing the following roles and responsibilities while keeping in mind that the specifics may vary to best meet individual firm needs.

ATTORNEY TEAM

Attorneys are often the first to have discussions regarding receiving client ESI. Attorneys should bring their litigation support colleagues into these discussions as early as possible. It is critical that these discussions consider the IG implications of receiving client ESI, and that someone on the case team, ideally a project manager, coordinates with the appropriate teams including IT, litigation support, and records within the firm. In addition to the collection of relevant materials, the team needs to sort through how to track this material, the client's responsibility to retain a preservation set, and how to securely transmit the collection to the party processing the data and expected timeframes.

Attorneys, with the appropriate litigation support technical expertise, should also address the question of scope of collection with their clients. Some firms prefer to collect the minimum set of data believed to be necessary for the matter. Some clients, however, may prefer to over collect believing that to do so is more cost effective than having to perform subsequent collections due to a narrow scoping in the initial pass. The optimum approach will vary depending on individual circumstances, but the attorney on the case team is usually best suited to discuss collection approaches with the client. Similarly, attorneys should negotiate the scope and content of protective orders, again with an assist from litigation support on technical issues.

PARALEGALS

Paralegals play an integral role in the organization of the case file and tracking of all case materials including client ESI. As such, they often play the role of media manager. If the paralegal receives client ESI, they should coordinate with whatever team in the firm is responsible for importing and uploading the data, providing them access to the data if necessary, and any other relevant information (i.e., type of data, time sensitivity, etc.). Well-defined roles and communications between these two teams will ensure efficient processing of the data and potentially reduce the duplication of data. The team should avoid copying the data to a network share or other media storage device unless necessary.

eDISCOVERY LITIGATION SUPPORT

The eDiscovery litigation support team should assume responsibility for the data intake process. Even when they are not the first to receive the data from the client, they should be the first internal contact point. They should ensure the data is appropriately tracked and tagged. This team assesses next steps and gathers necessary information not previously provided. In conjunction with the records department, they should monitor chain-of-custody and ultimately retention and disposition of this content. These two departments should also collaborate to determine the best place to store this type of content. Finally, litigation support professionals will often be in the perfect position to help educate others not only on the how, but the why of good IG practices.

RECORDS DEPARTMENT

Historically, the records department has not often played a role in the lifecycle management of client ESI. However, the records department is best equipped to capture, track, monitor, and audit any actions that may take place with this critical data as it moves through the eDiscovery lifecycle. By partnering with the records department, firm personnel can access client ESI via the firm's records management system (RMS) (or similar platforms used for records management purposes). Such systems often offer robust capabilities to report on the location of data and provide an audit or history.

INFORMATION TECHNOLOGY

If maintaining any copies of client ESI in-house, IT plays a critical role in ensuring that the content systems that store and process ESI are available, have appropriate storage capacity, are performing acceptably, and are adequately secured. The help desk can also provide technical assistance for those accessing systems that contain client ESI. In some firms, IT may be responsible for ensuring that a given data store is appropriately associated with a client or matter number and what IG guidelines are involved with procuring this storage.

VENDOR MANAGEMENT AND PROCUREMENT

Some firms have a dedicated vendor management or procurement department. These individuals should be engaged in the vendor vetting process and assist in ensuring that contract terms are consistent with firm policy and practice for storing, retaining, backing up, and handling other security and IG requirements.

CLIENT

Often, the client will dictate IG requirements for the firm. For example, a firm must honor a client's data retention policies for copies of client ESI, especially if they are more aggressive than the firm's default policy.

RISK MANAGEMENT/GC

The risk management team, or General Counsel, will help define the firm's risk tolerance, a key factor in determining processes and procedures, and will lead the effort to identify IG requirements that apply to ESI.

BUSINESS DEVELOPMENT

Business development will often have a stake in retaining client ESI to facilitate competing for new cases. It is important to balance the firm's business development needs, with IG concerns aimed at managing the firm's retention, compliance and risks associated ESI.

A PROPOSED DATA INTAKE AND TRACKING PROCESS

We recommend firms document and implement a data intake and tracking process (DI&T process) to properly govern client ESI. This is critical because client ESI may come to the firm via the lawyers representing the client, without other stakeholders being aware or involved up front. Accordingly, a standardized DI&T process endorsed by litigation department heads and communicated to and understood by all members of a firm's litigation team, is critical to ensure that client ESI coming into the firm is appropriately tagged and tracked from receipt until disposition. The process should be consistently adhered to, and exceptions should only be permitted in extenuating circumstances with documentation. This section outlines key elements of a DI&T process for firms to consider when developing their own process to improve governance of client ESI.

STAKEHOLDER ROLES

Typically, the litigation support team plays the key role in client ESI intake, but is often dependent on other case team members to ensure they are aware of incoming client ESI. All case team members must be educated as to the proper routing of client ESI. For example, clients may directly email ESI to an attorney or paralegal on the case team. The recipient needs to know to whom the client ESI should be forwarded for proper intake and tracking according to the firm's approved intake process. Firms may also choose to educate their clients as to the preferred method of ESI transmission (some firms will discourage the practice of clients transmitting ESI via email to ensure that ESI is kept out of the messaging system).

INITIAL DATA INTAKE

Firms receive client data in a variety of formats and on various forms of media. During initial intake, firms should catalog the source media so it can be tracked. All attorneys and staff who may receive or otherwise come in contact with client source data should know which team is responsible for initial intake and the process required for getting the data to them.

There are several options for tracking source data. A best practice employed by some firms is to make a copy of the data upon receipt and route the source media to the firm's records management function, where the media can be scanned into the RMS and physically stored in a controlled environment. The existence and storage location of the copy is also noted in the RMS. Other firms may use eDiscovery software packages that include media tracking functionality to track the source data in the same system that will contain subsequent iterations of the data created during review and analysis. At a minimum, a firm should have a tracking log, even if that takes the form of a spreadsheet, with the appropriate columns necessary to establish chain of custody. Regardless of the tracking tool used, firms should identify the data with a client or matter number, description of the data that includes marking it as client ESI, date received and firm custodian. A sample of a simple tracking log can be found in Appendix A.

As a best practice, all firms should limit the number of approved repositories in which to store, review and analyze client ESI. These may be internal systems or external repositories hosted by third party vendors. Again, this information must be circulated to all members of a firm's litigation case team to minimize the chances of attorneys or staff storing data in a location that is not properly tracked for client ESI purposes.

Sometimes, firms will make a copy of the raw data received from clients and destroy or return the source media to the client. This decision may vary depending on the size of the data and other circumstances. It is critical to record in the chosen tracking tool whether the source media is returned, destroyed or retained.

TRACKING CLIENT ESI

After the client source ESI has gone through initial intake, copies will begin to proliferate. These could be working copies made during the intake process, copies made at ingestion into a review tool or during early case assessment, or other similar processes. Tracking can be complex, as these copies may reside on internal systems or on an outside vendor's system. The firm will search, sort, tag, analyze, and produce the data, using various eDiscovery tools and may create several additional copies in altered states. Tracking each and every copy is an important part of the DI&T process.

Chain of custody is an important concept that must be applied to the process of tracking client ESI. Controlling who has access to client ESI, documenting the movement of client ESI between individuals and systems, as well as any changes, establishes a defensible chain of custody necessary to prove the integrity of the data if required to present the client ESI as evidence before a court of law.

Typically, the litigation support team will work with the records management team to develop an effective scheme for tracking each new iteration. Date of creation, custodian, media or system containing the copy and a description should be recorded. The description should note that the copy is client ESI, how the data has been altered from previous iterations, and whether any firm work product has been introduced. As with the intake of the initial source data, the existence and locations of these additional copies should be noted in the RMS to facilitate management throughout the data lifecycle.

During the course of litigation, the opposing party, or third parties, may produce data that will be contained on source media, copied, and even loaded into review systems. Much like other data sources involved in the eDiscovery process, the firm should track the intake of data provided by opposing parties or third parties as part of a litigation.

The types of information tracked by the firm should be similar to those tracked for client provided ESI.

INFORMATION SECURITY — DATA INTAKE

To appropriately keep information secure, it is important to understand what type of data is being received, and what IG requirements must be enforced, be it regulatory requirements, client requirements, court ordered requirements or even firm requirements.

Identifying this data appropriately may be easy if, for example, the client is a hospital and routinely identifies when the data provided contains protected health information (PHI). Often, clients will have only a very general idea of the type of data contained within the provided ESI, and just as often, the amount of data precludes either the client or the firm from properly triaging the data, making it very difficult, or practically impossible, to accurately classify the different types of data during the intake process.

Ideally, a firm would only need to receive collected data likely to be relevant. Both clients and firms would benefit from assembling a checklist that targets the types of data required for various types of litigation. Firms could even offer to work with clients to create a data map that aids in more targeted collection.

Another possibility is that firms could use technologies similar to those found in data loss prevention (DLP) tools, which could scan a collection and identify the types of potentially sensitive information within the collection. There are tools available today that are very accurate when searching for sensitive information such as social security numbers or account numbers, however finding more amorphous types of sensitive information is more problematic, but the tools are getting better every day.

Realistically, at least for the foreseeable future, many clients and firms won't have the time or technology to fine-tune their collection efforts. In these instances, a best practice might be to identify a standard of data security that the firm believes comfortably fulfills its obligations in most cases. Such a standard would likely include:

» **Encryption of copies of client ESI made upon intake.**

» **Physically securing original source media containing client ESI.**

» **Restricting access to client ESI by default, and only granting access on a need basis via access control lists.**

» **Setting up monitoring and auditing on data stores containing ESI.**

» **Ensuring processes are in place to actively remove the rights of users who no longer need access to client ESI - one technique is to generate a charge back to the legal team for each allocated named user license.**

Because these requirements can be difficult to implement on all systems, it is important to limit the systems that can contain client source data. For example, accepting client ESI as an email attachment may be convenient, but makes the data both hard to track and secure as described above. Another example: using public file shares to store received ESI without appropriate tracking is also very convenient, but also poses problems for tracking, securing, and managing the data.

Firms should develop a single method for electronically receiving information that utilizes systems that can be appropriately secured, such as secure file transfer. Regardless of source, data should be kept in a repository where it can be associated with a client matter. To control the more convenient, but less manageable data stores, firms will need to implement policies describing how to appropriately use such systems, audit processes to find data that may be already on these stores, and enforce methods such as quotas. Educating users on what they have to do, and why it is important for both the client and the firm is the key to success.

THE DATA INTAKE AND TRACKING PROCESS AND KEY IG PROCESSES

This section places our processes discussion and recommended best practices in the context of the key processes discussed in the 2012 Symposium report.[2] We explore how several of the key IG processes relate to, and can assist, firms in the tracking and disposition of client ESI.

RECORDS AND INFORMATION MANAGEMENT (RIM)

Records management processes can be used to assist case teams and litigation support staff in the tracking and disposition of client ESI. For example, firms that use RMS to manage records retention can use the same system and protocols to calculate and enforce retention periods for client ESI. Records management and litigation support staff should be familiar with the broad principles and processes relevant to both disciplines to ensure that client ESI is managed appropriately.

DATA RETENTION AND DISPOSITION

Data retention and disposition are core processes within IG. However, for those that deal with client ESI, data disposition poses significant challenges. For many lawyers and firms, keeping all litigation data is a standard practice to guard against the chance that the case can come back to life. Firms' business development departments might also be opposed to deleting ESI since having that data may reduce client costs and give the firm an advantage when competing for additional business. In recent years, client-imposed outside counsel guidelines have obligated firms to return data to the client at the conclusion of a matter. (Please see the 2014 "Emerging Trends Task Force Report: Outside Counsel Guidelines Management: An Information Governance Issue."[3])

If all client ESI is returned at the conclusion of a matter, does the firm then have an incomplete matter record? Striking a balance between a "complete" matter file and a "sufficiently complete" matter file is challenging. When the time comes to dispose of or return data, the process may be complicated, especially in systems that contain both client ESI and firm work product. Those systems often don't have the ability to be granular enough to treat firm work product and client ESI differently. Disposition of matters may also be complicated by IG itself. For example, if a matter is under a protective order, the people typically charged with disposition of the data may not be able to view it.

Firms must also address what options to provide the client upon disposition. Typical options include return, destroy, or transfer to a new matter. These options can be complicated by technical challenges, such as providing data from a litigation support system in a format that will be usable by the client either now or in the future, especially if the client doesn't have the same system or doesn't support standards such as Electronic Discovery Reference Model (EDRM), XML. Finally, when thinking about disposition, firms must consider both revenue and billing challenges. Should they (or can they ethically) charge for retaining this data after the close of the matter? And if so, what is the best approach for billing? To deal with many of these challenges, it may be necessary to build a case for applying retention and disposition processes to ESI.

Retention of ESI

Four potential approaches to retention of client ESI exist. Determining the most appropriate approach should involve consideration of several factors. These factors include the nature of the case, the likelihood of an appeal, and the client's satisfaction with the firm's handling of the case as well as the outcome secured. Should a dissatisfied client question the handling of client ESI during the preparation or execution of the case, the firm may be called on to defend decisions and judgments associated with the inclusion or exclusion of ESI. Finally, the firm's relationship with the client may play a role in determining the appropriate retention of the ESI for the completed matter. Long-term clients are often granted services not typically offered by the firm.

Retain Everything

There are many potentially valid reasons to retain all ESI upon the close of a matter. As mentioned previously, it may be in the firm's and client's best interests to maintain ESI that is likely to be involved in future litigation, as a cost and time saving measure. The firm's risk management team may specify that all case ESI is to be kept for an appropriate amount of time to cover potential malpractice claims. Statutes of limitations for litigation cases range from 5 to 12 years, depending upon the state in which the case was litigated. Most firms, for reasons cited previously in this paper, increasingly recognize that risk and costs associated with retaining all ESI for all cases isn't cost effective and are trending away from this approach.

Retain Items Produced

Different types of ESI may permit varying retention periods. For example, ESI collected, but determined not to be relevant in a case may have a much shorter retention period than ESI produced to opposing counsel or other parties.

Retain Admitted Items

For some cases or clients, the firm may opt to retain only those items of ESI admitted in the legal proceeding.

Retain Nothing

The firm may elect to place the entire obligation for storage and retention on the client. The firm should communicate and document the retention obligations to the client. The firm may also require the client to agree to permit the firm access to the ESI should the firm have a need to do so.

THE CASE FOR MANAGING ESI DISPOSITION

Holding on to data indefinitely poses many risks to the firm. Many of these risks are well known to IG professionals, since they are similar across all types of data the firm maintains. Risks and considerations are outlined below. However, developing and implementing standard operating procedures, checklists, and matter lifecycle workflows can minimize exposure and reduce expense associated with over-retention of client ESI. Conducting a conference with the case team and other key support personnel as soon as the matter has concluded should be considered a best practice. It is at this conference that ESI can be appropriately inventoried and disposition decisions can be made.

Firms must establish a disposition process for client ESI. In most cases, the options for disposition of ESI will be similar or identical to the options for dealing with a client's file. For example:

» Transfer to New Matter

The eDiscovery data may be applicable or responsive to a new active matter. The challenge will be determining and segregating the files to be transferred and taking appropriate action for any remaining files.

» Archive

As a service to the client and a business development strategy (as having the data may lead to additional work), the firm may opt to store the data for a specific period of time. Many firms charge the client for this storage. Archiving client ESI should be done with consent from the client to avoid creating issues relating to the client's records retention policies. Firms should also set up procedures for archiving that consider requirements for security, tracking, management, and eventual disposition of the data being archived. For example, it may make sense to exclude backup media as an archive source, since this media might make eventual disposition of the data much more difficult.

» Deletion

In consultation with the client, the firm may elect to delete the data generated for the matter, including client-provided ESI.

» Return to Client

Some lawyers will determine it appropriate to return client-owned ESI and other materials to the client for storage or destruction. When doing this, firms should consider keeping copies of key data that might be required to respond to future client questions or to protect the legal interests of the firm. A recommended best practice is to offer client ESI materials back to the client at the end of a matter, so the client can choose to keep it for possible use in a related case.

DATA VOLUME

Even the smallest case can involve the processing and review of thousands of documents or emails. Additionally, the eDiscovery process may result in the creation of many additional copies of client-provided data. While disk storage may be "cheap", the processes to support managing this storage are not. For example, for every terabyte of data a firm stores, they must allocate additional storage and expense to make sure the data remains available in the event of equipment failure. The data must be backed up and managed in case of catastrophe requiring disaster recovery. Outsourcing these functions or sending them to the cloud typically only shifts the costs since most of these providers charge based on the amount of storage in use.

LIABILITY FOR THE FIRM

Retaining client-provided ESI for use in connection with a particular matter, after the close of that matter, unnecessarily obligates the firm to be responsible for records that do not belong to the firm. In addition, holding on to client ESI may raise conflict issues for the firm on future matters. Another consideration is that retaining client-provided data for use in connection with a particular matter after the close of that matter may present a conflict with a client's records retention schedule, or violate provisions of the client's outside counsel guidelines. Finally, retaining client ESI may pose a risk for both the client and the firm if ESI must be preserved and eventually reviewed as part of new litigation. This becomes especially problematic if there was no business or legal reason to retain that ESI, especially if it should have been destroyed in normal course prior to the existence of the new litigation.

FORMER CLIENTS

Without an effective IG process, some firms may find themselves holding data long after the client relationship has ended. During this time, individuals may die or organizations cease to exist or become acquired by another entity. All of these events make eventual destruction or return to the client much more difficult and expensive.

PROCESS FOR DESTRUCTION OR RETURN

The process to either destroy data or return it to the client is very similar to the review process required when returning the client file to the client. However, depending on the type of data involved there are deviations from the client file review process. The process should consider all sources of ESI under control of the firm, including those maintained by third parties such as vendors who are hosting ESI for review.

Collected Data

Collected ESI, be it on source media provided by the client, or copies which have been unaltered by processing can be returned to the client or destroyed without additional review, since these files contain no work product.

Processed Data

Collected data is typically modified with software that culls the data by search terms, extracts metadata, or provides information to the legal team to make an initial data assessment. Processing the data also creates files that allow the resulting ESI to be loaded into a review platform. Although the output from processing is very useful while a given matter is still in progress, it can typically be considered as transitory when a matter is closed. In most cases, this data can be destroyed as part of the disposition process.

Review Platform Data

Data retained in a review platform includes both ESI and information about how that ESI applies to the matter. This latter category can include document coding for relevance, privilege or issue, attorney notes about the case, information about redactions, and other case related information. Because such a database combines work product created by the firm with client-provided documents, the firm's review notations and coding of client-provided data may include attorney notes or comments not intended for the client. This poses a disposition challenge, since it often isn't feasible to separate the work product from the client-provided data. Further, in many jurisdictions the entire database could be considered part of the client file. This issue becomes more complicated if the review platform is hosted by a vendor, since the firm may want to keep a copy of this information for a period of time after matter closure, even though the client may want to discontinue vendor fees immediately.

Returning this data to the client can pose a challenge if the client intends to ever use the data in a review platform. Standards such as EDRM XML may help with data exchange, but clients should still expect potential issues loading the data into a new review platform, with the risk increasing as time passes. It is important that you involve the firm's risk management team when formulating procedure for handing review platform data disposition.

Produced Data

Often, during the course of a matter, the firm creates one or more "production sets" which will contain ESI, or documents based on the client's ESI. These production sets are typically part of the client's file, but can be returned or destroyed, depending on the firm's retention obligations, without review.

Opposing Party Data

During the course of litigation or investigations, the opposing party, or third parties, may produce data that will be contained on source media, copied, and even loaded into review systems. This type of data is typically considered part of the client file, but can be returned or destroyed, depending on the firm's retention obligations, without review.

DATA REMEDIATION AND SPECIAL CONSIDERATIONS FOR DECOMMISSIONING REPOSITORIES

The considerations outlined so far in this section have a common requirement: the firm must know the location and type of data associated with a given matter to exercise appropriate disposition procedures. However, this will not always be the case. Data remediation, the process of identifying data that existed prior to the establishment of DI&T processes, could easily take up its own paper. We will, however, address a special case of data remediation – the decommissioning of a litigation support repository.

A litigation support repository may be a collection of loose files on a share, an old review system where cases are being allowed to age off, old processing systems, or custom built databases. Such repositories may house large amounts of legacy data that does not easily lend itself to data retention best practices. If data in repositories can be classified by client or matter and source data, it should be handled in accordance with the firm's retention policies. However, data in these repositories may contain various types of unstructured data that cannot be classified by data type or by client or matter. When faced with a huge challenge, the best approach is often to take small steps to solve the problem. For example:

» **Involve records management, eDiscovery litigation support teams and client teams. Working together, they may be able to use a combination of institutional knowledge about the data source and firm retention policies to identify some of the data.**

» **Explore using technology to potentially identify or classify unstructured data. For example, keyword searches may allow loose files to be associated with a client, an internal client team, or even a specific matter.**

A firm's eDiscovery litigation support team may have access and expertise in using such technology.

- Involve your risk management team to develop strategies and approval processes for data that cannot be easily associated with a matter. Focus on general rules that can apply to any repository and any data type. Set general retention guidelines that follow firm's general retention policy against the age of the data.
- For data that must be retained but cannot be migrated to a successor repository, the retention method and the storage medium for the data after the repository is decommissioned should satisfy the firm's cost and IG requirements. Here are some example issues and factors to consider when making these decisions:
  - Migration to a new litigation repository that supports all of the firms IG requirements may be ideal, but the cost may not be justified for inactive matters.
  - If the data is to be archived, the archive should be tracked using the same DI&T process discussed earlier in this paper.
  - The firm's high performance storage area network may provide the fastest access to the data, but because the data will rarely be accessed, this may be considered too costly.
  - Storage on DVDs is very inexpensive. But retrieving the data for potential use later may be much harder, and expensive manual processes would be required to search the data.
  - When choosing how to best archive such data, the firm should also consider the longevity of the source media, the usability of the data stored on the media in future litigation, and the ability to apply governance to the data in accordance with the firms IG policies.

IT SYSTEMS ADMINISTRATION

In addition to handling storage capacity planning, availability, and performance, IT staff can be critical in helping to track and control unstructured data sources that contain client ESI copies. They can also help facilitate secure transfer of client ESI copies. IT also enforces who has access to the data on certain types of systems or data stores.

MATTER MOBILITY

The client file transfer process should include client ESI. When transferring litigation matters to another firm, if client ESI exists, it should be reviewed to remove firm work product and notes from the data transferred. However, this may prove challenging as discussed in the next section. For a discussion on matter mobility, see the "Matter Mobility Task Force Report."[4]

DOCUMENT PRESERVATION AND MANDATED DESTRUCTION

Any information that is potentially relevant to an ongoing litigation must be exempt from destruction procedures. The team responsible for administration of legal holds must understand the process to communicate with the records department, or other teams responsible for overseeing document disposition, so that items subject to litigation hold are exempt from destruction.

The process for returning documents under litigation hold may vary depending upon the nature of the hold. In some cases, the firm may require that copies be made before releasing documents to the client. Firms should involve their risk management teams before deciding how to release records associated with litigation holds.

Clients, litigation opponents or others may seek to impose on a firm an obligation to dispose of eDiscovery data deemed to be confidential business information. Firms should only agree to dispose of documents that the firm is not otherwise obligated to hold by applicable law, court order, regulation, rule, or an existing firm document hold or preservation order to retain. Firms should resist proposed protective orders or agreements under which the firm would be required to dispose of documents that would otherwise be defined as the firm's official records, particularly to the extent that the documents in question reflect work product of the firm as opposed to confidential documents supplied by another party.

A firm's risk management team should be consulted about the terms of a proposed protective order that would require the disposal of documents other than discovery materials or other copies of pre-existing documents received from a client or third party. As a final check, the firm should make sure that what they agree to is technically feasible without causing disruption to firm operations. For example, for many firms, it is not possible to return or destroy all copies of client documents within 30 days of matter closing if such destruction includes back-up tapes, legacy litigation support systems, or other sources of "dark data." In this event, the firm could propose to keep such information secure until it can be reliably destroyed.

THIRD PARTY RELATIONSHIPS

When engaging a third party vendor to assist with the collection, processing, review, or production of ESI, a firm should have a defined vetting process to track the data maintained by a third party vendor, to support auditing capabilities and ensure compliance with any applicable guidelines. Such guidelines can be the firm's guidelines, a client's outside counsel guidelines, and regulatory guidelines such as HIPAA (for more on HIPAA requirements, see the "HIPAA Omnibus Task Force Report"[5]) or the needs of the specific matter. Firms may consider entering into master service agreements (MSA) with select pre-vetted vendors to lessen the time required during the vendor selection process. As part of an MSA, a standard engagement agreement that will be used for each matter, a template statement of work (SOW) should be considered for incorporation as attachments to the MSA. The MSA typically sets forth the working relationship between the firm and the vendor, while the engagement agreement and SOW set forth the specifics for the matter at hand. During the vetting process, the firm should examine the vendor's processes and protocols for data intake, data security, data transport, and data disposition processes to ensure they are compatible with the firm's IG standards. A basic vendor-vetting checklist is provided as part of Appendix A, and examples from other sources such as ARMA and Sedona are referenced in the bibliography.

DATA INTAKE AND STORAGE

When selecting data intake and storage, a firm should ask the vendor to walk them through the specific steps of their evidence check-in process, including chain of custody procedures. It is important to consider all the ways in which the vendor could potentially receive the evidence including physical media, via secure file transfer, etc. This process should conform to both the firm's and the client's standards for the specific type of evidence. It is important to confirm the vendor's policies regarding where and how data is stored (both the physical source media and any resulting copies) also conforms to the policies of the firm and the client. For example, country specific laws prohibiting data movement outside of the country's borders could cause problems if the vendor plans on storing client ESI outside of the ESI's country of origin. The firm should also ascertain how processed data is hosted. For example, if data is stored in a remote cloud, how is data from one case segregated from data of another case? It is also important to consider the pricing implications of the chosen data storage. Does the vendor charge a storage or hosting fee for source media after a certain period of time? How is data that was loaded into an early case assessment platform charged? For vendor hosted review tools, the firm should consider instructing clients to send the data directly to the vendor, removing the firm from the chain of custody.

THIRD PARTY INFORMATION SECURITY

Working with the firm's IT, data security or procurement team, the firm should understand the vendor's specific information security procedures and consider including the vendor's security protocol as an attachment to their matter specific engagement agreements. This protocol should outline the overall security protocols the vendor has in place. If not specifically covered in the security program documentation, a firm should inquire about:

- **Disaster recovery plan including recovery time objective (RTO) and recovery point objective (RPO)**

- **Backup procedures**
- **Data breach policy**
- **Data privacy policy**
- **Data encryption protocols**
- **Data retention policy**
- **User access control policies**
- **Any recent security audits by a financial institution or independent auditor**
- **Details and resolution of any breach within the last five years**
- **Reliance on other vendors including cloud usage**

In addition, if the firm has the opportunity to perform a site visit of the vendor's facility, it is strongly recommended to proceed with the visit. While on the vendor facility tour, it is important to note: 1) the physical security of the facility, 2) how people and packages are granted access and logged into the space, and 3) the security procedures required when logging onto computers.

DATA TRANSPORT TO A THIRD PARTY

It is important to understand your vendor's capabilities and protocols regarding the transmission of data generated by the systems they use to support your matter. These should be covered in the data encryption policy provided during the vetting process. When transferring data on physical media outside the four walls of the vendor's facility, it is recommended the vendor encrypt the data using industry standard encryption software to secure the contents of the media. If the firm has a data encryption policy in place, you should consider asking your third party vendor to abide by the firm's policy. While the encryption process potentially adds time to a given request, the benefit of securing the data likely outweighs the additional time and inconvenience of working with an encrypted container.

THIRD PARTY DATA DISPOSITION

As part of the disposition process it is important to consider all sources of data that a vendor may have worked with including:

- **Physical media from collection**
- **FTP or other secure data transfer tools**
- **Unprocessed source data copied to a vendors staging area**
- **Processing database(s)**
- **Review database(s)**
- **Production output**
- **Transcript management systems (hosted vendor solutions or reporting company websites housing transcripts and exhibits)**
- **Trial presentation systems**
- **Near or offline storage**

When considering disposition or mobility of the data, it is important to consider the pricing implications of the various options for disposition. As part of the engagement agreement process, the pricing for database export, archiving, standard deletion, or certified destruction (including documentation) should be established.

INFORMATION SECURITY

Security of client ESI is of the upmost importance to the firm and its clients. Lawyers safeguarding client data is a basic tenet of their professional responsibility as members of the Bar.[6] As defined by U.S. Code, the term information security means "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction."[7] Client ESI can include sensitive information such as a client's intellectual property, trade secrets, other proprietary information, and other regulated information such as personally identifiable information (PII) or protected health information (PHI). Due to the increased spotlight on information security, it has become a crucial factor in determining the continued growth, or even existence, of a client relationship.

INFORMATION SECURITY AT THE CLOSE OF A MATTER

Client ESI that is retained should be kept at least as securely as when it was in active use, using the best practices outlined in the data intake sections above. Some clients, regulations, or court orders will require that client ESI be destroyed within a typically aggressive period of time. When the data is on servers and subject to backups, this may not always be easy or feasible. Also, as discussed in the matter retention and disposition section, it is important these destruction considerations are vetted prior to the legal team consenting to avoid having attorneys agree to something that isn't practical or advisable.

INFORMATION SECURITY PROCESSES THROUGHOUT THE EDRM

While only one component of a broader IG strategy, keeping data secure throughout the eDiscovery lifecycle may be among the most visible components, there are many security impacts on how data is handled at each stage.

Most firms do not become the custodian of client ESI until the client has finished the collection process. In the data intake section above, we discussed several best practices as client ESI enters the firm. Below we will discuss information security for the other stages in the EDRM.

PROCESSING, REVIEW AND ANALYSIS

As client ESI is processed, culled, analyzed and hosted for review, it will typically move through various systems and storage platforms. Ideally, data copies that are redundant should be deleted as soon as possible. If there are business reasons not to delete these copies, they should be identified and tracked for retention purposes as discussed in the previous DI&T process section.

For these eDiscovery platforms, many of the same security best practices identified in data intake apply. For example, firms should grant rights to access review platforms only to those personnel that need access. As personnel working the matter change, access rights must be updated as well. Removing the rights of people who no longer need access to the review platform is especially important.

For matters where the firm successfully identified sensitive data, or if there are known client or regulatory guidelines, any person granted access to the platform should be immediately informed about the nature of the IG requirements and educated on best practices. It is important to note that many of these requirements will impose a higher standard than the attorney's ethical requirements around confidentiality.

Many firms will use contract attorneys to review client ESI. It is important that these contract attorneys be bound to the same information security policies and processes as the firm's attorneys and that they are educated on the same best practices. If they are independent contractors, they should be contractually bound to honor the IG requirements of the matter. This should be in addition to any requirements imposed upon the vendor providing the contract attorneys.

For IT, it may not be feasible to encrypt client ESI hosted in a review system. However, any data time client data is transported it should be encrypted. For example, when firms put client data on portable media, whether for backup, archive, or transport, it should be encrypted. Likewise, if a portable hard drive contains processed client data to be loaded on a third party hosted review platform, the media should be encrypted prior to transport.

PRODUCTION

For many reasons, it can be difficult to secure client ESI during production. The first reason is that production is often done under great duress, as deadlines approach and the additional security procedures can take extra time. The second reason is that the adverse party may not be interested in cooperating with the additional procedures involved to receive secure data. The third reason is that attorneys often don't want to deal with the hassle of encryption or secure transport. In some instances, the review team or technology can help by redacting information that might be sensitive or protected by regulation or client requirements. However, since many times neither the legal team nor the litigation support team knows for certain if the production set contains sensitive information, the safest route is to encrypt the media used to transport the produced data. Education and reminders help gain attorney cooperation. If possible, work with the risk management team to enact a firm-wide policy requiring written approval for exemption from encryption.

PRESENTATION

As the team goes to trial or arbitration, they will often have a subset of client ESI on their laptops, on portable hard drives, or similar devices. They may have a war room set up in a conference room or a hotel containing a small network to allow the trial team to operate remotely. Because of the high pressure and fast paced environment that often goes along with a trial, information security is often the first causality. However, the risks at trial can be even greater than during the eDiscovery process because of the chaos that often accompanies trial support. A best practice is to assign responsibility to a trial team member to ensure all security protocols are followed. Examples of such security protocols include confirming all team members are encrypting all media, physically securing client ESI when not in use, avoiding short cuts and convenience steps which significantly compromise security such as sharing passwords, and ensuring that once the trial is over all materials are securely returned to the appropriate systems.

CONCLUSION

We hope this paper provides a starting point for firms who have not yet grappled with managing client ESI as part of a larger IG program, as well as providing some practical tips for firms who have already started that journey. While there are important nuances, we believe solutions and processes for managing the client ESI IG problem can be found in the careful and appropriate implementation of a sound IG program across the entire organization.

REFERENCES

1. *Building Law Firm Information Governance: Prime Your Key Processes; July 2013, Iron Mountain Law Firm Information Governance Symposium.*
http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/B/Building-Law-Firm-Information-Governance.aspx

2. *A Proposed Law Firm Information Governance Framework; August 2012, Iron Mountain Law Firm Information Governance Symposium.*
http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/A/A-Proposed-Law-Firm-Information-Governance-Framework.aspx

3. *Emerging Trends Task Force Report: Outside Counsel Guidelines Management: An Information Governance Issue; July 2014, Iron Mountain Law Firm Information Governance Symposium.*
http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/e/Emerging%20Trends%20Task%20Force%20Report%20Outside%20Counsel%20Guidelines%20Management

4. *Matter Mobility Task Force Report; July 2014, Iron Mountain Law Firm Information Governance Symposium.*
http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/M/Matter%20Mobility%20Task%20Force%20Report

5. *HIPAA Omnibus Task Force Report; July 2014, Iron Mountain Law Firm Information Governance Symposium.*
http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/H/HIPAA%20Omnibus%20Task%20Force%20Report

6. *American Bar Association;*
http://www.americanbar.org/aba.html

7. *US code 44 U.S.C. § 3542(b)(1)*

8. *The Sedona Conference Commentary on Information Governance.*
https://thesedonaconference.org/publication/Best%20Practices%20for%20the%20Selection%20of%20Electronic%20Discovery%20Vendors

BIBLIOGRAPHY

ARTICLES

The Sedona Conference Commentary on Information Governance
https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Information%20Governance

Big data, big problems: as the risks of handling big data grow, information governance is an important legal & technical issue
Author(s): Mike Brown and Ramin Tabatabai
New Law Journal. 164.7598 (Mar. 14, 2014): p21. (UK publication)
http://www.newlawjournal.co.uk/nlj/content/big-data-big-problems

Information Governance Best Practice: Adopt a Use Case Approach
26 November 2013 (Gartner)
Massive data growth, new data types, litigation, regulatory scrutiny and privacy/information risks have all created an urgent need for information governance. IT professionals considering MDM, eDiscovery, information archiving or cloud migration should start implementing information governance now.

Information Governance Even More Important in the Era of Big Data
November 7, 2012
http://www.forbes.com/sites/barrymurphy/2012/11/07/information-governance-even-more-important-in-the-era-of-big-data/
In the Big Data era, where companies are able to quickly make sense of larger quantities of data than ever, information is finally recognized as a critical business asset. But too many companies are on the "Big Data Bandwagon" without even a thought of how it could affect eDiscovery costs or risks.

The Impact of Information Governance Trends on eDiscovery Practices in 2014
March 13, 2014
While information governance (IG) may be a gigantic, broad category, GCs and CIOs were hit with a startling realization: For their organizations to significantly reduce eDiscovery costs they must proactively manage electronic information at an enterprise level. This starts with information governance.

Leveraging Big Data for Litigation Readiness and eDiscovery Success
ILTA, 2013
Discusses how to leverage technology to achieve effective litigation management.

eDiscovery: Where We've Been, Where We Are, Where We're Going
Peck, Andrew J.; Facciola, John M.; Teppler, Steven W.
12 Ave Maria L. Rev. 1 (2014)

Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing
Rashbaum, Kenneth N.; Borden, Bennett B.; Beaumont, Theresa H.
12 Ave Maria L. Rev. 71 (2014)
http://heinonline.org/HOL/Page?handle=hein.journals/avemar12&id=77&collection=journals&index=journals/avemar#77

Advice from Counsel: Trends That Will Change eDiscovery (and What to Do about Them Now)
Kaplan, Ari L.
12 Ave Maria L. Rev. 109 (2014)
http://heinonline.org/HOL/Page?handle=hein.journals/avemar12&id=115&collection=journals&index=journals/

avemar#115

Information Governance: It's a Duty and It's Smart Business
Charles R. Ragan,
19 Rich. J.L. & Tech. 12 (2013),
available at http://jolt.richmond.edu/v19i4/article12.pdf.

The Compliance Case for Information Governance
Peter Sloan,
20 Rich. J.L. & Tech. 4 (2014
http://jolt.richmond.edu/v20i2/article4.pdf.

Finding the Signal in the Noise: Information Governance, Analytics, and the Future of Legal Practice
Bennett B. Borden & Jason R. Baron,
20 Rich. J.L. & Tech. 7 (2014)
http://jolt.richmond.edu/v20i2/article7.pdf.

Building a Successful eDiscovery Strategy
Information Management, November-December 2013
http://imm.arma.org/publication/frame.php?i=183189&p=34&pn=&ver=flex

A Roadmap to Litigation Readiness: RIM Staff Help Navigate the Way
Information Management, September-October 2012
http://content.arma.org/IMM/Libraries/Sept-Oct_2012_PDFs/IMM_0912_Legal_Watch_Litigation_Readiness.sflb.ashx

BOOK

Information Governance: Concepts, Strategies, and Best Practices
By Robert F. Smallwood
Published April 2014
Available via Amazon
Information Governance (IG) is a rapidly emerging "super discipline" and is now being applied to electronic document and records management, email, social media, cloud computing, mobile computing, and, in fact, the management and output of information organization-wide. IG leverages information technologies to enforce policies, procedures and controls to manage information risk in compliance with legal and litigation demands, external regulatory requirements, and internal governance objectives. Information Governance: Concepts, Strategies, and Best Practices reveals how, and why, to utilize IG and leverage information technologies to control, monitor, and enforce information access and security policies.

GLOSSARIES

THE SEDONA CONFERENCE GLOSSARY:

eDiscovery & Digital Information Management (FOURTH EDITION)
The Sedona Conference, 2014
Source: https://thesedonaconference.org/
A glossary to assist in the understanding and discussion of electronic discovery and electronic information management issues.

Glossary of Records and Information Management Terms (4th Edition)
ARMA International, 2012
Source: http://www.arma.org/
A glossary intended for anyone working in records and information management. Terms from numerous disciplines are included: records management, archives, , legal services, and business management.

REPORTS (for purchase)

Worldwide Information Governance and eDiscovery Infrastructure 2013-2017 Forecast
May 2013
Source: http://www.idc.com/getdoc.jsp?containerId=241218
Price: $4500 (18 pages)
This IDC study reviews the state of the eDiscovery infrastructure market in 2012 and provides IDC's revenue forecast for 2013–2017.

eDiscovery and E-Disclosure 2013: The Ongoing Journey to Proactive Information Governance
https://451research.com/report-long?icid=2295
This report examines the state of the eDiscovery market, including the impact of assisted-review technologies, data-privacy regulations and the explosion of big data
$3750

APPENDIX A

FORMS, TOOLS, SAMPLES AND GUIDELINES

Simple tracking log for data intake process

TAG NUMBER(S)	SERIAL NUMBER	DESCRIPTION	DATE COLLECTED OR TRANSFERRED	MAKE/MODEL	DATE/TIME	RELEASED BY	RECEIVED BY	REASON

VENDOR VETTING CHECKLIST

I. POTENTIAL VENDOR VETTING QUESTIONS:

A. INFORMATION ABOUT YOUR COMPANY

1. Name of company (and of parent if a subsidiary). List subsidiaries for which you are the parent.

2. Describe your company's business (general terms).

3. What is the nature of the company's ownership? (Partnership, Corp, etc.).

4. List the names of the company's leadership team (or principals) including titles.

5. How many years has your company been in business under its current name? Please list other company names and years in business if applicable.

6. List eDiscovery services provided by your company. Include number of years for each service offered. Please highlight any special services you offer which we may be unaware of (e.g., Cyber Security Consulting, Mac data/iDevice collection/processing, cloud media preservation/collection/processing, uncommon mail format processing).

7. List the location of your offices and facilities and describe whether the location is a project management, sales or production facility.

8. Outline and explain the types, purpose, and amount of insurance(s) carried, licenses and bonding your company holds.

9. Are any of your services subcontracted to other vendors? If so, what services and what vendors?

10. Are any of your services performed off-shore? If so, please explain.

11. What third party software vendors do you have strategic partnerships with? Please describe any such relationships.

12. Has your company, parent or subsidiary been named, either as sole or codefendants, in any civil suit generated by your past or current operations? Have any legal judgments or settlements been made against your company, parent or subsidiary in professional or general liability cases within the last five years? If so, please provide information (circumstances, award amounts, decisions, etc.) on all cases.

13. Within the last five years, has the company or its parent ever filed for bankruptcy or met the criteria for bankruptcy?

14. Are you currently involved in any business-restructuring transactions or discussions with other organizations, including acquisitions or divestitures?

15. Outline and explain licenses, certifications, credentials and other distinctions your company holds.

16. Describe your enterprise-wide client and matter conflict process.

17. For each office and facility, fully describe your physical and technical security measures with respect to data protection, hardware integrity, building safety, and third party outsourcing.

18. Describe your company's disaster recovery plan in sufficient detail to assess the comprehension of the plan.

19. Do you have a fully enabled back-up site? Explain the data replication/mirroring process and intervals as well as the criteria for and speed of the fail over process.

20. What is your data backup strategy, procedure, and recovery process in the event of hardware failure or data corruption? How long are such back-ups retained?

21. Is there a law firm client-facing portal available? Can one submit work requests? Does it track job requests/monitor status? Is it a ticketing system? Does it do anything else? Is it updated in "real time"?

22. Describe your company's conflicts check process.

B. INFORMATION ABOUT YOUR COMPANY'S ESI COLLECTION

1. Does your company provide an ESI collection? If not, skip this section.

2. Please provide a description of your firm's chain of custody tracking procedures, your collection cataloging inventory procedures, and documentation of collection activities.

3. How many engineers/technicians are directly/indirectly employed by your organization to do on-site collection of ESI?

4. Please list the relationships/strategic partnerships you have with other collection services, and the number of engineers for each such relationship or partnership.

5. Do your collection technicians/engineers undergo a certification process? What certifications do they hold?

6. Have your directly/indirectly employed engineers/technicians testified (via deposition, affidavit, or court room) about an ESI document collection project?

7. For the international ESI collections, please indicate whether your technicians/engineers are U.S.-based or whether they are foreign-based. If they are foreign-based, are they certified?

8. Do you outsource your international ESI collections? Please list the relationships you have with foreign-based ESI collection companies.

C. INFORMATION ABOUT YOUR COMPANY'S ESI PROCESSING

1. What backup tape formats/types can your company restore with its internal resources?

2. What software do you use to process ESI?

3. What is your data processing and loading throughput/capacity?

4. Do you perform a virus scan on ESI as part of your processing? If viruses are detected, can you clean the virus without modifying data or metadata?

5. Explain your procedures and processes for ESI processing that ensures preservation of original data and metadata throughout the entire process.

6. Please describe your approach to data QC (including handling of exceptions and typical exceptions workflow). If there is a time out feature in the data processing tool, please explain the exceptions workflow related to this.

7. What data minimization options are available to us (ECA, EDA etc.)?

8. Please describe your approach to TIF/image QC.

D. INFORMATION ABOUT YOUR COMPANY'S ESI REVIEW TOOL(S)

1. Do you store any amount of client ESI in the cloud?

2. Do you host the online review tool(s) yourself or do you partner with another party? If a partner, please name them.

3. What is the name(s) of your online review tool(s)?

4. Does your review tool(s) support the review of foreign language documents? If yes, which languages?

5. Does your review tool(s) allow searching in foreign languages?

6. Are any of the search features unavailable when searching foreign language documents? If yes, which ones?

7. What technology assisted review (TAR) options are available to us?

8. Are the social networking graphics from emails available to us?

9. Please describe how automated, random sampling strategies are built into your processes?

10. Please give us details how you are able to process and handle for review "structured data," to the extent not otherwise described elsewhere. Please give at least one example of a structured data project you've handled.

E. SECURITY PROTOCOLS

1. Please describe your disaster recovery plan and the extent that you'd like to include a copy of your plan, please do. Please include descriptions of your recovery time objective (RTO) as well as your recovery point objective (RPO) in this context.

2. Please describe your backup procedures if not already covered in the disaster recovery plan. Please describe the most amount of work that would be lost in a critical failure.

3. Please describe your data breach policy if not already covered in your security plan.

4. Please describe your data privacy policy if not already covered in your security plan.

5. Please describe your data encryption protocols if not already covered in your security plan.

6. Please describe your data retention policy if not already covered in your security plan.

7. Have you undergone a security audit by a financial institution, independent auditor or other?

8. Please list any certifications that your company has and when achieved.

9. Please give us the details on your data transfer protocols.

10. Do you certify data destruction? Do you generate a certificate without being prompted? How much does the certificate cost? How do you address destruction of data on backup tapes/media archive?

F. PERSONNEL

1. Please give us an organizational chart listing senior and technical positions (including testifying experts).

2. Please give us the number of project managers, analysts and developers, and whether they are based in the U.S. or a foreign country.

3. Do any of your project managers have certifications or specialize in specific types of cases/products/strategies?

4. What is the average tenure of your employees?

5. Do you ask your employees to sign confidentiality agreements?

6. Do you run criminal background checks on your employees?

G. PREVIOUS PROJECTS

1. Please list the work performed by your company for our firm in the last 18 months. Also add the names of your firm's contacts for each project.

H. REFERENCES

1. Please provide a list of three law firm references who have used your eDiscovery offerings in the past 18 months.

II. THINGS TO LOOK FOR IN AN SITE VISIT TO A PREFERRED VENDOR:

A. DATA PROCESSING FACILITY

1. Please make notes on the "physical security"

   a. What type of security is there to enter the space?

   b. Is it easy for "tailgaters" to gain access?

2. Ask about the Media/Evidence check in process

   a. Suggest they run you through the process of their evidence check-in

   b. Be sure that they cover the chain-of-custody procedures

3. Tour

   a. Ask for a tour of the space

   b. Ask for introductions to staff members

B. DATA CENTER

1. Please make notes on the "physical security"

   a. What type of security is there to enter the space?

   b. Is it easy for "tailgaters" to gain access?

2. Please ask to see the UPS devices and make notes on what happens in the event of a power failure

3. Tour

    a. Please ask for a tour of the space

    b. Please ask for introductions to staff members

C. DOCUMENT REVIEW SITE

1. Please make notes on the "physical security"

    a. What type of security is there to enter the space?

    b. Is it easy for "tailgaters" to gain access?

2. Tour

    a. Please ask for a tour of the space

    b. Please ask for introductions to staff members

3. Please ask for review and take notes on the ability to communicate with other offices (client).

4. Please make notes on whether there is adequate kitchen/lounge space.

5. Please make notes on the capacity (per room and total).

6. Please ask how different projects in the same space will be "walled" off.

7. Please make notes on the desktop configuration for the average coder (dual monitors, etc.).

For more information, the Sedona Conference[8] has a "best practices" for the selection of eDiscovery vendors.

SAMPLE LANGUAGE FOR THE CLOSING LETTER

Re: Conclusion of Representation

Dear:

We are writing to confirm that our representation in connection with [describe matter] has been concluded, and that our representation of you, therefore, is ended. Because the lawyer-client relationship between us has ceased with respect to this specific matter, we will have no further obligation to advise you in connection with this matter or as to future legal developments that may have a bearing on the matter.

At this time, we have closed the file pertaining to the matter or sub-matter. Upon request, we will return any original documents and other property you provided to the firm in connection with the representation. Our file pertaining to the matter or sub-matter, which might include, for example, firm administrative records, time and expense reports, personnel and staffing materials, credit and accounting records, and internal lawyers' work product such as drafts, notes, internal memoranda, and legal and factual research, including investigative reports, prepared by or for the internal use of lawyers, will be retained by the firm according to our retention period. For various reasons, including the minimization of unnecessary storage expenses, we reserve the right to destroy or otherwise dispose of any such documents or other materials retained by us, without further notice to you in accordance with the firm's record retention policy.

We are pleased to have had the opportunity to be of service to you, and we thank you for asking us to do so. Should there be matters in the future where we might be of assistance again, we hope you will call upon us, and we shall be pleased to consider possible retention with respect to those matters.

Sincerely,

Attorney

Xxx/yyy

SAMPLE ENGAGEMENT LETTER LANGUAGE FOR LIT TECH DISPOSITION

Conclusion of Representation; Retention and Disposition of Your Documents. Unless previously terminated, our representation of [client] in any matters on which we perform services on behalf of [client] will terminate upon the date we last render services. At that time, we will close the matter file.

If you have provided us with documents in paper or electronic form as part of a litigation matter, we reserve the right to destroy these in accordance the firm's record retention policy for client- provided documents. Upon request, we can instead return any original documents and/or other property you provided to the firm in connection with the matter.

WORKFLOW FOR HANDLING EXTERNAL MEDIA

INTRODUCTION

External media containing electronic information for litigation support arrives to the firm on a regular basis. It may be associated with a file arrive with a file transfer, or be sent directly from the client or by a third party for an active litigation the firm is already handling. In addition, while media may be sent directly to those responsible for litigation support, it could, and very often does, get sent directly to the legal team handling the case. To efficiently maintain the integrity of the chain of custody and track the media a repeatable process should be implemented and followed.

EXTERNAL MEDIA INTAKE

All external media received by the firm should be processed by the staff assigned to handle incoming electronically stored information (ESI). These individuals will identify the appropriate department to process the data. In some cases, external media may be tagged with a client/matter number and unique ID before being forward for processing.

External media received by anyone in the firm that is identified as production data should be forwarded to litigation support that will:

1. Label external media with the following information:
    a. Type of data (matches document categories used in other systems)
        i. Client Documents: Any original client documents, emails, word docs, etc.
        ii. Discovery: Any vendor disk containing the processed data of those client documents
        iii. Production Document: Any document that was produced to the other side or the other side produced to us.
    b. Client/Matter name and numbers
    c. Bates or control numbers
    d. Date
2. Load the data into the appropriate repository
3. Forward the external media to the Records Management Department for storage

The Records Management Department will:

1. Index the external media into the Records Management System (RMS) under the appropriate client/matter under the category identified by litigation support.
2. Print and adhere a barcode to the media or media case.
3. If barcode is placed on the case, using a permanent marker, print the barcode number on the physical media.
4. Assign to a fireproof/lockable media box obtained from your off-site storage vendor.
5. Send the media box to the off-site media storage using established Records Department procedures for notifying the vendor and securing media storage container.

CONSIDERATIONS:

1. Matter Mobility – Incoming ESI should be reviewed on intake.

   a. Track chain-of-custody: Incoming external media should be reviewed and identified with a unique ID number and the client/matter number when received.

   b. Confirm firm's authorization to have the data (i.e., have conflicts cleared, engagement letter in place, etc.).

   c. Only after the data has been verified should it be forwarded to litigation support for processing.

      i. Track circulation and ensure external media is placed in secure media storage.

REGISTERING DATABASES IN RECORDS MANAGEMENT SYSTEM

TRAINING GUIDE

The process outlined in this guide is for general training purposes only. Process for specific matters should be tailored based on the unique requirements of that matter.

Purpose

The purpose of this document is to provide training on using [RMS] to track creation of litigation support databases.

Applicability

The process outlined in this document is designed to be used on projects where litigation support databases are created.

Timing

This process should be used at the time that the litigation support database is created.

Responsibilities

The Project Manager/Coordinator or Analyst creating the database is responsible for creating the [RMS] entry. This should be done for all types of databases including Relativity, Concordance, Case Notebook (LiveNote), LAW, Trial Director/Visionary, and CaseMap/TimeMap [REPLACE THIS LIST WITH YOUR FIRM'S LITIGATION SUPPORT SOFTWARE].

Process

The process of registering the database is comprised of the following steps:

This guide assumes that the eDiscovery/Litigation Support personnel will be doing the data entry. Instruction may be as simple as stating "contact your Records Department."

1. **Logging in**

2. **Creating the entry**

The instructions below outline this process:

Instructions:

1. **Logging In**

   » [ADD INSTRUCTIONS FOR ACCESSING RMS AND LOGGING IN – SCREEN SHOTS HELPFUL]

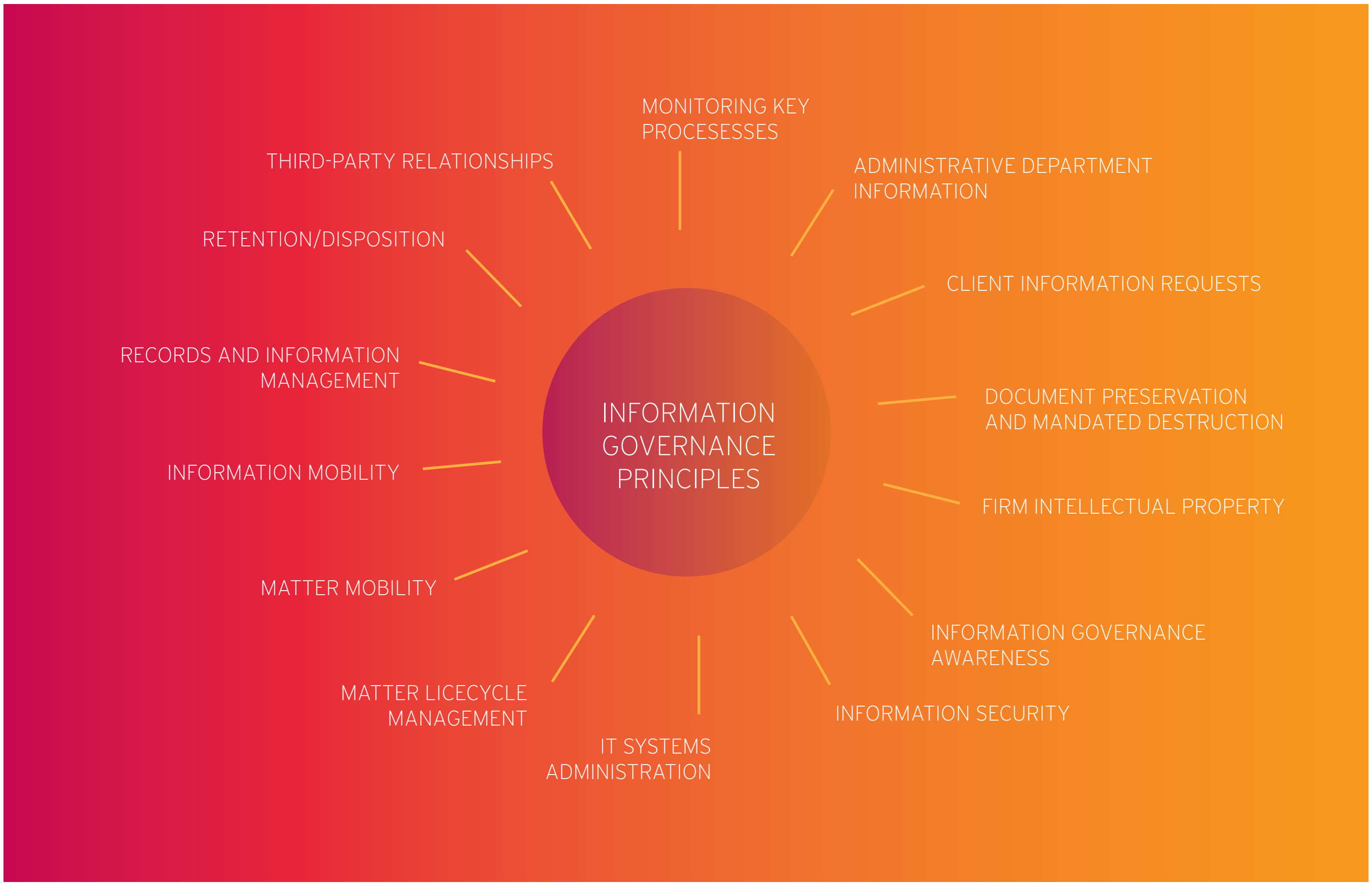
2. Creating the Entry

   - » [ADD INSTRUCTIONS FOR CREATING AN ENTRY] (Best Practice is to add a folder/media type specific to databases.)

   - » [ADD STEP FOR ENSURING ENTRY IS BEING CREATED UNDER APPROPRIATE CLIENT/MATTER NUMBER AND FOLLOWS ANY OTHER AGREED UPON CLASSIFICATION/CATEGORIZATION]

APPENDIX B

LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM – IG FRAMEWORK AND KEY PROCESSES


INFORMATION GOVERNANCE PRINCIPLES
MONITORING KEY PROCESESSES
ADMINISTRATIVE DEPARTMENT INFORMATION
CLIENT INFORMATION REQUESTS
DOCUMENT PRESERVATION AND MANDATED DESTRUCTION
FIRM INTELLECTUAL PROPERTY
INFORMATION GOVERNANCE AWARENESS
INFORMATION SECURITY
IT SYSTEMS ADMINISTRATION
MATTER LICECYCLE MANAGEMENT
MATTER MOBILITY
INFORMATION MOBILITY
RECORDS AND INFORMATION MANAGEMENT
RETENTION/DISPOSITION
THIRD-PARTY RELATIONSHIPS

KEY PROCESS DESCRIPTIONS

1. Administrative Department Information – The process of managing the law firm's internal strategic and operational business information, including the preservation of vital records to ensure business continuity.

2. Client Information Requests – The process of managing the law firm's internal strategic and operational business information, including the preservation of vital records to ensure business continuity.

3. Document Preservation and Mandated Destruction – The process of preserving potentially responsive information, ensuring the suspension of scheduled disposition, and certifying custodial legal hold compliance during the discovery phase of litigation, investigations, or audits. Also the destruction of information as managed by the court or by agreement among parties.

4. Firm Intellectual Property – The process of capturing and preserving the firm's knowledge and operational, creative, and historical artifacts the hold commercial, business, or strategic value (e.g., marketing and branding materials; KM resources; contact information; firm initiative planning information; business development strategies; firm strategic plans; case management strategies; lateral lawyer growth records; financial information; firm policies and procedures).

5. IG Awareness — The process of providing guidance, proactive education, and training to frontline support and local office administrators.

6. Information Security – The process of controlling access to information, for example, via ethical walls and confidential access controls. It includes the protection of personally identifiable information (PII or PHI) and confidential client information and remote access to systems.

7. IT Systems Administration – The process of providing guidance on systems selection and implementation, database administration, commissioning/decommissioning/ developing systems, and information migration.

8. Matter Lifecycle Management – The process of capturing new or new matter information that is organized by areas of law and/or practice groups, including client engagement documentation and perpetuating the collection/distribution of firm authoritative information. The process of systematically deactivating matters in firm systems at the conclusion of formal representation (matter closing) is a part of this umbrella process.

9. Matter Mobility – The process of moving matters and their associated information into and out of a law firm; triggered by lateral moves, client terminations and other events.

10. Information Mobility – Information mobility is the process of providing guidance and compliance with firm policies/procedures, with respect to acceptable storage, use and security of client information, on both firm-issued and personally owned devices.

11. Records and Information Management — The process of applying lifecycle management practices to client and firm information, to enact disposition as authorized, and apply defensible disposition to legacy information.

12. Retention/Disposition — The process of creating and periodically revising operational guidelines for managing information assets at the law firm, including file folder structures and taxonomy.

13. Third Party Relationships — The process of ensuring consistent contracting language and defining Service Level Agreements that are compliant with firm policies regarding information access and protection.

14. Monitoring Key Processes — The process of regular monitoring and evaluating key information governance processes to ensure that the organization meets the goals of the program. This involves establishing operational metrics and benchmarks to evaluate the overall effectiveness of the IG program.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.