IRON MOUNTAIN®

STRATEGIES FOR COLLABORATION SITE GOVERNANCE IN LAW FIRMS

2021 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

This paper is dedicated to our friend and colleague, Rob Weaver. His collaborative spirit, passion for sharing his knowledge and contributions to our industry leave a great legacy.

AUTHORS:

KAREN ALLEN, CIPT
Information Governance Manager
Wiley Rein LLP

REGGIE POOL
Senior Director, Information Governance
HBR Consulting

TERRENCE J. COAN, CRM
Managing Director, Information Governance
HBR Consulting

SAMANTHA LOFTON MOSS, IGP
Chief Risk, IG and Legal Project Management Officer
Ice Miller LLP

DANA C. MOORE, IGP, CEDS
Director of Risk Management
Hinshaw & Culbertson LLP

STEVE HUFFMAN, CRM, IGP
Director of Strategic Solutions – Records & Information Governance
Williams Lea

BRYN BOWEN
Practice Group Leader - Legal Risk
Intapp, Inc.

DOUG SMITH CIGO IGP
Senior Records Manager
Crowell & Moring LLP

SCOTT CHRISTENSEN
Vice President
Qualitest

MADELEINE LA COUR, IGP
Director, Business Intake and Records
Baker Botts LLP

KELLY F. FARMER
Director of Information Governance
Latham & Watkins LLP

ANGELA STROUD AKPAPUNAM, IGP, CISM
Director, Information Governance and Records
WilmerHale

ANDREW FREEMAN, IGP
Global Information Governance Operations Manager
Latham & Watkins

INTRODUCTION / PROLOGUE

Collaboration – (noun) - [kuh-lab-uh-rey-shuhn] - Collaboration is the act of working together, especially on a goal or shared project, often used in a positive context to refer to two or more parties successfully working together on professional or artistic projects. It often implies not just cooperation but the sharing and development of each other's ideas. In recent years, the legal ecosystem has seen a rise in the use of collaboration tools. Those tools enable coordinated workflows by providing a unified platform for discussion, file sharing task assignments, and real-time project collaboration.

Collaboration software can come in many forms, but at its heart, it is all about aligning people to provide firms with an ability to better serve and communicate with their clients. For the law firm, implementation drivers can range from internal needs to client demands, and the various tools available provide a range of features and functionality. Whether a platform is required by the client or provided as an in-house solution, each stores information differently and may require a unique Information Governance (IG) approach.

Collaboration is more than file sharing; it's more than just chat and real time communications and co-authoring. It can be any one of these, or any combination of these, and more. It is important to note that not all applications that incorporate these features are identified as collaboration platforms.

Depending on a firm's specific configuration of features, a collaboration platform could be used for only one or two capabilities, such as to share files. Not all features are available in all solutions, so firms need to consider the purpose of the collaboration they are looking to implement.

The content in this paper is a combined effort of our team of authors. It includes a set of considerations extracted from the experience and interests of the group as a whole, broken out into individual "articles" that address areas of interest in the use of collaboration tools from a law firm IG professional's perspective, no matter which collaboration platform is selected. The sections vary in topic and length, but each is intended to stand alone as well as in unison, to guide the reader to their conclusions. We feel this format allows the reader to focus on topics that are most relevant to their situation. In some cases, themes may overlap and ideas repeat. When there is an opportunity to reference other sections that provide greater detail, those have been identified and links provided if you are reading this electronically.

We have tried to be consistent with our nomenclature, but please bear in mind that the various platforms can refer to the same features using different names, while some platforms use the same term for different features. When we refer to a team, we are not necessarily referring to MS Teams, but the concept of a shared collaboration space.

CHOICE OF COLLABORATION TOOLS

THE RISE OF COLLABORATION SOLUTIONS

Let’s take a look at the rise in the use of collaboration tools in the legal industry, both at their current levels of use and their potential future applications.

A common reason for the increase in use of collaboration applications is to replace and/or supplement the in-person interaction of knowledge workers. More recently, for many firms, the distancing restrictions brought on by the COVID pandemic escalated the pace of adoption. Remote collaboration was seen as a quickly viable replacement for in-person interaction, whether it was as a structured meeting platform or an informal idea exchange medium.

In addition to the rapid replacement focus, the versatility and flexibility of many collaboration platforms have exposed other expanded use cases. Chief among these is as a centralized knowledge platform (or in Microsoft parlance when discussing Teams, a “single pane of glass”) that can incorporate the use of many programs from a single platform. For example, Zoom has an MS Teams add-in on its platform in addition to a plethora of project and content management applications. MS Teams has a fully developed ecosystem of not only MS applications, but many of other business-related programs. This ability to leverage multiple applications with another individual or group, in context, and from a single platform is a key benefit of any platform choice.

CHOOSING THE RIGHT SOLUTION

One of the main considerations in choosing the appropriate collaboration platform is the degree of functionality, business responsiveness and usability of a tool evaluated against the complexity of implementation and maintaining the content from a governance perspective. Firms should consider their potential use cases, and whether there is a single solution that meets their needs or if multiple platforms may be required. For example, does the firm need a deal room, somewhere to share files, project management functionality or co-authoring capabilities? Each of these may indicate a different solution and different set of potential IG considerations. For example, MS Teams implementation must be a thoughtful, planned venture because of the potential governance challenges inherent in such a cross-functional platform, particularly when planning where content is stored. If not done properly, it can create tension between functionality and governance, which may ultimately undermine both user acceptance and functional resilience.

What are some of the primary factors to consider in choosing the right collaboration platform for your firm? Is the tool a replacement for an existing solution or is the tool meant to provide a new way of working? Here is a list of considerations (not necessarily in order) to help you and your leadership make that decision:

- Security - Does the hosted environment meet firm and client security requirements? A full-blown security assessment (e.g., SIG Lite) should be conducted before using any collaboration platform.
- Functionality - Does the platform offer the range of functions necessary to meet the firm's objectives?
  - How effectively does it aid collaboration?
  - Can it successfully replicate in-person interaction?
  - Is the level of interaction sufficient in a hybrid working environment where some participants are in person and others are virtual?
  - Can it provide a sense of (virtual) community?
- Ease of use, user adoption and user compatibility - How intuitive is it to access the platform and its functions?
  - How many steps and what degree of training is required to access key functionality?
  - Is the platform's functionality responsive to the user's needs? Remember, too much software is generally not a good thing for lawyers.
- Access rights management - For law firms, confidentiality, ethical walls and outside counsel guidelines requirements are all considerations.
  - How easy is it to maintain an evolving set of access instructions, centrally, to ensure consistency and compliance across all platforms?
- Scalability - Can the platform accommodate expanded use with minimal reconfiguration?
- Ease of deployment and maintenance - Will your existing internal IT and IG teams be able to implement and maintain the platform with relatively few resource enhancements?
- Governance considerations - To what degree is the firm willing to spend time and resources to ensure that the content management (storage, accessibility, security, disposition) schema is coherent and effective?
- Cost - Firms should address the cost aspect of a platform in terms of the TCO "total cost of ownership", including the degree of implementation, training, maintenance and governance aspects. As an example, MS Teams is part of the MS 365 bundle therefore many firms are already paying for the appropriate software license, but their licensing level may not include all features that a firm may require. Cost considerations also go well beyond licensing.

- Implementation and management - Particular attention should be given to the configuration and management of information repositories. Modern collaboration solutions are delivered via a SaaS model that allows the firm to focus on configuration and strategic use.
    - What are the costs associated with the implementation and long-term management of the product?
    - Do you require additional headcount or a new skill set that requires additional training?
    - What are the potential e-discovery benefits or risks?

SUMMARY

The rapid adoption of collaboration tools is driving firms to reassess their current content-sharing and communication solutions. As the market responds to the need for collaboration solutions, new products continue to enter the marketplace. The selection of an appropriate solution for your firm requires the development of a full set of use cases along with both technical and functional requirements. Firms must keep in mind that as their implementation progresses, requirements may change and new features may become available that will require additional IG considerations. With appropriate rigor and considerations, such as those listed above, the time and effort required for the selection and implementation of a collaboration tool can be optimized.

WHO GOVERNS THE SPACE

As with many Information Governance (IG) challenges, a central question to answer is who governs the collaboration space. The entity that governs the space is responsible for making critical decisions in several areas that include security, access management, and retention and disposition. Governance of collaboration tools requires cross-functional ownership and involvement. Key players include IT, IG, Information Security, Compliance, Knowledge Management, Privacy – and the business. IG should have direct input to the administrative controls governing the collaborative space to ensure that proper controls are in place. Some questions to ask are:

- Who can make disposition and retention decisions?
- What are the impacts of outside counsel guidelines (OCGs)?
- How are litigation holds implemented and maintained?

In many situations, the answer to these questions depends on who owns the content. Law firms are often the custodian, not the owner, of the information. In most cases, IG practitioners should look to the local regulations and requirements where a firm operates for guidance.

ACCESS REQUIREMENTS

If the law firm hosts the collaboration space, then they are responsible for governing the access to, and security of, the shared information. Access should be controlled, as appropriate, for different categories of users. Internal users may have greater access than client users or other groups outside your organization. Sections of the collaboration space could be open to clients and internal users. You may also need/want to define unique access to spaces for those outside both your and the client's organizations (for example, experts or co-counsel).

Practitioners may want to provide segregation of proprietary information of the law firm by having different access rules for certain parts of the collaboration space. This allows for discussion of the business of a representation (staffing, budget, client relation) within the collaboration space without inappropriately exposing proprietary information. The firm and client may have a separate chat and messaging space for privileged discussions. A repository for shared information resources could be shared with all groups, firms, clients and other outside users.

EXTERNAL COLLABORATION SPACE CONSIDERATIONS

> IT IS IMPORTANT TO HAVE A DEFINED APPROACH TO DATA THAT IS IN FIRM-CONTROLLED CLIENT COLLABORATION SPACES VS. A CLIENT-CONTROLLED COLLABORATION SPACE.

A client-owned collaboration space, where the client has invited the law firm to share documents in their hosted space, has a certain risk in that the firm may not have the rights to download content or preserve information in the collaboration space. As a best practice, law firms should have established guidance and procedures for its users on how to preserve data. It is optimal for the firm to host the space for various reasons, such as privileged communications and the ability to preserve work product and client documents.

One safeguard a firm can deploy is to include language in the client engagement letter regarding security concerns related to the use of their collaboration space. The law firm should instruct firm employees to save all content uploaded to a client site into the law firm's DMS (or another official repository for the matter). See the Disposition section for considerations relating to client vs. firm ownership of records.

Additional topics for consideration that may be relevant depending on whether the space is client- or firm-hosted:

- Accessibility and Access controls Accessibility and Role-based Access Controls (RBAC)
- How and where to save work product
- Controls on what users can see and download
- Preservation strategies
- Backups and other copies
- How to manage content (chats / posts / documents)
- Written policies and documented procedures
- Training materials and instructions (how to work in the firm's collaboration spaces)
- E-learning guides, FAQs, etc.
- Help desk or assigned group gets requests for collaboration sites
- Client-facing protocols/checklist:
    - access controls, parameters for sites, and how-to tools/reference guides.

SUMMARY

Who provides this governance? In most cases, the host bears the responsibility whether it is the firm or client. It is highly recommended that you address these issues with the appropriate attorneys in order to outline best practices for using collaboration sites at your firm, as found in the other sections of this paper, including Managing for External Guests.

PROVISIONING

By standardizing the provisioning of new working spaces within a collaboration tool, rather than letting users direct all aspects of creation, a firm can ensure that all content in the tool is associated with a client or administrative matter number. Having a client and matter number associated with content ensures that it can be governed by all relevant policies throughout the lifecycle of the data. In turn, users should have the ability to request new spaces associated with client and matter numbers if there isn't a mechanism in place to automatically create an associated space.

RESPONSIBILITIES

Ideally, the ability to provision teams is a process that is controlled by an administrative group that considers all factors related to security, privacy and Information Governance (IG). This group would be responsible for creating a system of naming conventions, metadata and templates for use in creating new teams in a standardized way. Once conceived, the process of handling team requests should be automated as much as possible. The development of an exception workflow is also recommended for scenarios where the need for a new team does not fit neatly into a predefined template. The exception workflow should include an escalation group that includes staff with IG expertise to make recommendations about custom team settings to accommodate exception requests.

INTEGRATION WITH DMS OR OTHER SYSTEM OF RECORD

All created teams have some analogous considerations that necessitate similar settings. Firms need to be able to govern content in the tool, whether that means defining the tool as an approved repository, linking to other systems, migrating to the system of record or retaining in place. Integration with the firm's system of record, most often the firm's document management system (DMS), is one of the most vital. If the firm has a DMS that includes matter-centric workspaces, one approach would be to ensure that all provisioned teams have a corresponding workspace or folder in the DMS. Integration with the DMS provides the ability to use the DMS as an overlapping repository that facilitates the management of content, including preservation and eventual disposition. A third-party tool or internally developed API may be necessary for this integration, in addition to any automation of the provisioning process.

TEAMS TEMPLATES

The types of templates needed to standardize provisioning in a collaboration tool generally fall into three categories:

- **Client and/or matter level:** will likely make up a majority of the collaboration spaces created in a firm and are used to facilitate work for specific matters. Some applications limit the number of workspaces you can have at any one time. This may alter the design and decision process around the creation of client matter-specific spaces. For instance, with MS Teams, you are limited to 500. In this instance it may be better to have a client-level team with matter-level channels that could have different levels of security depending on the need.

- Additional considerations with client matter spaces include items like access controls (security) and disposition. For client matter workspaces, content should be made private while still allowing users to search and request access, equivalent to integration with the firm's ethical wall solution. For retention, many platforms have built-in disposition workflows based on automatic time-based content deletion. These settings are not ideal when the firm wants to implement disposition dependent on a trigger associated with matter close.

- **Administrative:** correspond to functional, departmental or geographic administrative groups. Privacy settings of the team should correspond with the access setting specified in the DMS and other repositories related to the group. These teams should be associated with administrative matters that have routine departmental retention disposition review, and may be good candidates for automatic time-based content deletion.

- **Project-based:** are often administrative in nature and cross-departmental. Multiple department and matter numbers may be associated, and possibly needed, to consolidate in some way. A department owner should be named for the admin site, and while other administrative department users may have access, the owner would be responsible for managing access and retention review. The creation of a project team may be needed in conjunction with the use of project management software, which could be integrated into the associated team. These teams are also good candidates for automatic time-based content deletion.

SUMMARY

Establishing an effective provisioning process is key to the lifecycle management of a collaboration space. While native functionality in a collaboration tool may be adequate for provisioning workspaces for most organizations, the specific requirements of a law firm justifies the identification, selection and implementation of a law firm-specific collaboration management solution in order to support its requirements for ethical walls, security, matter centric content control and support for multiple practice areas through templates and customization.

MANAGING ACCESS

MEMBERSHIP / ACCESS FOR FIRM-HOSTED SPACES

A firm should have overarching policies and procedures in place that govern the formal provisioning and management of any new workspace. The site requester or owner must adhere to these policies when defining the access and security requirements for the workspace, including the roles and responsibilities of both internal and external participants (guests).

Provisioning policies and procedures should define who grants access and who administers collaboration sites. If an organization has multiple tools, the administrators should work with users to determine the best tool for the use case in order to ensure selection of the appropriate application. A workflow should be defined for site access requests and approval for new members.

Routine compliance reviews of sites should be conducted during which site managers must affirm users who should still have access to sites and remove users who have left the firm or should no longer have access for other reasons. These reviews apply to both internal and external site members. External guests who are no longer affiliated with a member organization should be removed immediately.

Items to consider:

- Site Access Request and Evaluation
  - Documented contact for each site: external lead/owner and internal lead/owner.
- Site Audits
  - Approvals for new members
  - Removal of internal members who have left the firm or external members no longer connected with the site
  - Updates based on need-to-know access: transfers within the firm (admin or legal staff assignment changes)
- Rights Management
  - Level of access to sites (Private/View/Access Request)
- Walls
  - Ensure conflicts screens and ethical screens are observed
- Terms of Use
  - Internal users should be required to agree to terms regarding the use of the space and the potential sharing of content with external users

MANAGING FOR EXTERNAL GUESTS

Guest Terms of Use

The owner of the collaboration workspace should be responsible for ensuring all external guests are aware of, and understand, the guidelines for participation. It is recommended that all external guests be required to review and sign an agreement that clearly defines the guidelines for their participation. Some of the items to consider for collaboration site terms of use are (1) notice of site terms and agreement to terms by using the site, (2) routine review and attestation of users, and (3) notification of users who leave the organization. This list is by no means comprehensive but it is meant to provide a starting point for essential governance aspects.

Guest Policies and Procedures

A firm's Collaboration Workspace Policy should define those authorized to own, request and manage collaborative spaces in addition to the requirements for external guests. The Collaboration Workspace Procedures should provide clear instructions of steps that must be followed. Authorized external guests could be made to complete a Guest Information Form to collect the data needed to include them on the site. In addition, all external guests should be required to sign a Collaboration Workspace Agreement. These steps are required to ensure site security is maintained through dual-factor authentication. Information about a guest should include, for instance, the guest's name, contact information and role.

Guests Role-Based Access / Permissions

While each collaboration space or room may have a variety of roles (e.g., Administrator, Owner, Contributor, etc.) this section speaks specifically about the roles and responsibilities recommended for guests (i.e., external users).

- **Owner (Read/Write/Administrate Rights)**: guests are allowed to share/add content to the room. The guest can define if shared content can be edited, copied, or shared by others in the room or remain read-only.
- **Editor (Read/Write)**: guests that can edit some or all content in the room, depending on which folders/ collections and documents they have access to.
- **Read Only:** guests can view content and chat conversations but are unable to edit documents.
- **Commenter:** guests can comment in chat areas and or add comments about documents.

Guest Guidelines

External guests will need explicit access rights, typically in the form of a new account on the system defined by an administrator. Entry into the site should require dual-factor authentication. All external guests should be required to read and agree to Collaborative Workspace Guest Guidelines which can be included in the email invitation to join the site. The invitation should provide language similar to the following: "By using the site, you agree to adhere to all Collaboration Workspace Guest Guidelines". The following list of guidelines are suggestions and should not be considered all-inclusive:

- Guests are expected to respect the privacy restrictions set on the room. This includes not sharing their screen with users outside of the room participants to prevent the contents of the room from being seen, copied or used without authorization.
- No downloads or unauthorized screenshots of data are shared in the collaborative workspace. (Note: depending on the tool used, the collaboration space itself may have built-in functionality that would prohibit downloading any data)
- All comments on documents or chat areas are to remain professional and respectful of all room participants.
- Guests are responsible for providing notification to the administrator when members are no longer part of the team and/or should be removed from the space.

Guest Activity Audits

Firms should endeavor to ensure that all guest activity is subject to an audit. The audit should include content added, edits to shared content, and any attempt to print, screenshot, or download data to be reported to the room administrator. In addition, guest membership and verification of guest removal should be monitored. The firm's technology and IG teams need to work collaboratively to ensure that proper auditing is in place and that activity is reviewed regularly.

SUMMARY

While it is easy to get lost in the complexity of configuring access, one of the best use cases for collaboration technology is the creation of a shared workspace for collaboration technology with guests (e.g., external parties, partners and clients). While there is always an initial reluctance to give outside parties access to firm resources, current collaboration solutions provide several safeguards that, in combination with well thought out policies and procedures, can create a safe and productive environment that easily justifies the effort required to open up the collaboration solution to working with external guests.

REGULATIONS AND CLIENT REQUIREMENTS

If your firm plans to use a collaboration tool in conjunction with your representation of clients, there are several considerations concerning compliance with legal and ethical obligations, as well as client requirements.

DATA "OWNERSHIP" CONSIDERATIONS

One of the first things to consider is – who owns the data in the collaboration tool? Some clients may ask you to use their preferred collaboration tool in a platform that they "host."[1] If so, it is important to consider how you will keep a record of key documents that are generated and stored in that platform, as well as a record of your communications with the client. It is advisable to develop policies and procedures regarding any work product that might be primarily stored on a client system. One of the reasons lawyers maintain a file is to be able to defend their work if it is ever called into question. If attorney work product is stored in a hosted platform belonging to the client, it is possible that at some point in time you no longer have access to the information and do not have that critical evidence/data to defend yourself.

Alternatively, and more common, if you host the collaboration platform, you should consider how to maintain the client file – for example, will you move anything out of the tool and into DMS, and how will you apply retention periods in the platform. The good news is that a collaboration platform is typically a combination of solutions that you already manage (think remote access, document retention, instant messaging and acceptable use). Look to your existing policies and procedures to guide the management of this new solution.

LEGAL AND ETHICAL OBLIGATIONS

The types of clients you represent and the various laws and regulations that apply to them may affect whether and how you can use a collaboration tool.

Privacy Laws

There are several privacy laws (e.g., GDPR, HIPAA, CCPA) that could apply to the use of a collaboration tool, in particular related to the movement of data and security measures that must be taken concerning that data. You must ensure, for example, that you have the appropriate contracts or measures in place to allow the transfer of data outside the European Union in order to comply with GDPR. You must also make sure you are complying with any specific requirements in business associate agreements under HIPAA.

[1] The data is actually likely hosted in the cloud, but the platform is managed by the client.

Data Localization Laws

Some countries have data localization requirements. For example, China has a cybersecurity law that requires some data be stored in mainland China; Russia has a law requiring personal data is processed first in Russia before it can leave the country. Even the United States has export control laws, such as the International Traffic in Arms Regulations (ITAR), that restrict who can access protected data and from where. These laws may prevent you from being able to utilize collaboration tools to house data because they do not provide adequate security controls or controls over where the data is physically stored. It is therefore important to understand the type of data that users may put into the collaboration tool and to ensure that you are complying with any and all applicable laws.

Recording/Wiretapping Regulations

The use of recordings should be used thoughtfully. While recording is readily available in collaboration tools, it is important to note the feature falls under wiretapping and recording regulations in each state and most countries. Wiretapping covers both telephone and internet-based conversations.

For the U.S., each state is either a one-party or two-party consent state. More states are one-party consent states, meaning that so long as the participants know you are recording then that is sufficient. However, if any party being recorded resides in a two-party consent state, such as California or Florida, then you can run into problems. It is best to maintain transparency when recording meetings. Best practice includes verbal communication to all meeting participants that the meeting is being recorded, obtain each person's agreement to being recorded and use a recording notice banner (which is available on many collaboration platforms) as individuals enter the meeting.

Recordings can be discoverable. Make sure recordings are not happening just for the sake of recording if the conversation could otherwise have been discussed in-person or by phone in a confidential capacity. Do not say something in a recorded conversation that is confidential.

Consider a firm-wide policy about recording meetings and what types of meetings may be appropriate to record. Project meetings, for example, may be helpful to record if participants cannot always attend at the scheduled time, but a meeting with a client should seldom be recorded due to ethical reasons and American Bar Association advice.

It is helpful to be prepared with how you plan to respond upon entering a meeting that is recorded or if you are asked to consent to record a meeting. If you are hosting a meeting and someone does not agree to be recorded, be prepared to take good notes.

As with any information asset, be aware of what happens to recordings (e.g., where are they stored, who has access). Consider how long recordings should be preserved. Departments within a firm should create retention schedules that are simple enough for each team to follow, and address the specific needs of each team.

Ethical Walls

Access to information in collaboration sites is as relevant as it is in your document management system (DMS). Ethical wall access and restrictions should reflect across all data repositories. Aligning the membership of groups within collaboration sites to match access to information in DMS can be either a manual or an automated process. In either scenario, the decision-making is similar: which internal team manages access, and trues-up membership? A manual process is most certainly hard to keep up-to-date and some organizations are too large to scale. There are several tools on the market to achieve automation, however some of the tools require more technical expertise than others to establish.

Preservation Obligations

U.S. discovery obligations apply the same way to data stored in a collaboration tool as your DMS. Make sure you have a strategy and tools to implement a legal hold and to respond to a discovery request or subpoena.

CLIENT REQUIREMENTS, INCLUDING OCGS & CLIENT AUDIT FINDINGS

Another important set of considerations when using collaboration tools is whether any client requirements might restrict whether or how you can use them. These requirements might stem from Outside Counsel Guidelines or findings issued by the client's auditor. Relevant examples include requirements that you do not host data in the cloud, data loss prevention-related requirements or restrictions on where data can be stored geographically. Other examples include least privilege requirements – think about how you are going to build in a process to ensure this requirement is met. You may be able to leverage software (like ethical wall software) to help, but it is important to determine compatibility between systems. Even if you successfully find ways to use a collaboration tool and meet these requirements, it is also important to make sure you have the audit evidence necessary (e.g., detailed logging) for client audits.

SUMMARY

Given the substantial challenges surrounding compliance within an ever-changing regulatory environment, the management of the collaboration solution must be part of a firm's ongoing governance program. This is especially true when dealing with solutions that are SaaS-based, where changes to features and functionality happen frequently and often without warning. Ongoing review of both regulatory and client requirements, a necessary part of the firm's IG program, faces new challenges when addressing collaboration technologies, as information is centralized and rapidly collected across multiple mediums and shared across multiple parties which is the nature of the solution itself.

SYNCHING COLLABORATION TOOL CONTENT WITH YOUR DMS

WHY SYNC TO DMS?

For most firms, the DMS is the one source of truth for the client file. While the matter is active, legal teams may decide to use the DMS and collaboration tools interchangeably, or use one or another.   The ultimate goal is to ensure to the greatest extent possible that there are no lingering data sources to gather data for the client, court order, preservation hold, etc., and to minimize the spread of client information managed in multiple repositories.

TYPES OF SYNCHING TOOLS

Tools such as SeeUnity, Prosperoware CAM and Intapp Workspaces offer either one-way, bi-directional or real-time sync processes between several collaboration tools and the DMS.   Since this technology is very new to the market, be sure to fully understand the potential limitations before making a decision or implementing a solution.   Most document management systems are investigating native sync options, but the technology is currently still in its infancy and is largely being driven by the adoption rate of certain tools.

In any collaboration tool, version control is vital to keep files in sync. When multiple users work in both the document management system and the collaboration platform, it increases the risk of working off of an older or out-of-date version of a document which can be detrimental to a critical filing or submission.   Firms need to consider the available types of syncing to implement (one-way synch, two-way synch, working in the collaboration environment or the DMS) because versioning is not apples-to-apples. It is recommended to have a process where users work in one repository or the other.

SYNCHING TYPES OF DATA TO DMS

It is important to determine what types of files you want to sync to the DMS. For example, you may consider synching communication that is similar in nature to email exchanges (for example, the channel conversations in MSTeams) chat if it is retained and treated at the same level of importance as email communication. These communications may not sync to the DMS in native format but render as HTML files by date range or one .pst. The formats need to be tested to ensure they are searchable within the DMS, and in which format they can be exported for ingestion into eDiscovery tools, if required. Your firm may require communications to remain in native format within the collaboration site, and you have to establish the appropriate retention periods consistent with your firm's policies. There may also be specific file types associated with applications with video, reporting and other formats not appropriate or incompatible to store in the DMS.

WHAT DATA DO YOU WANT IN THE DMS?

At a minimum, information that is part of the complete client representation file should be included in the DMS. Any remaining content should have a retention period established that is consistent with your firm's document retention policy, or perhaps due to their nature, e.g. ephemeral posts and chats, be retained for some time consistent with statute of limitations and then deleted from the collaboration environment.

Administrative groups also use collaboration sites; their information should be synced to the DMS and retained consistently with your internal document retention policies. For administrative content, it may be more desirable that you only retain information required by regulatory and business requirements in the DMS, deleting remaining content and the site when no longer needed. Otherwise, you need to ask yourself these questions: Are you hosting this data indefinitely? Does it have a retention expiration? What data will be relevant 10 years from now?

CONCLUSION

Many view the rise of collaboration as a challenge to the standard legal DMS usage. Firms that have adopted the legal DMS as their one source of truth worry over the rise of yet another content repository under the guise of a collaboration solution. However, with an appropriate strategy and thoughtful technology adoption, a collaboration solution like MSTeams or Slack can be a DMS's greatest ally. As collaboration space takes the place of file storage areas and email, implementing a strategic plan for migrating content from the collaboration space to the DMS may mean more content ends up in the DMS than before.

DATA PORTABILITY

In addition to traditional electronic formats like document management systems (DMS) and litigation support databases, collaboration content is increasingly becoming commonplace for matter mobility. Cloud-based collaboration tools have multiple formats such as chats or instant messages, posts or conversations[2], notes, project files and shared office files. Moreover, some content may be stored in a location restricted to an individual user (e.g., OneDrive). The key to data portability is ensuring that these formats can be easily located and transferred for use in a variety of technical environments. The ability to export and maintain or "preserve" files in native format is important, and existing matter mobility policies should be applied independently of the format and medium.

IDENTIFYING THE DATA

It is essential to communicate early with stakeholders (i.e., responsible counsel, clients) to confirm the source, volume, timing and in what format the content will be delivered. If there is active collaboration, particularly with external parties, the target collaboration site (i.e., successor counsel or client's tenant) with appropriate access permissions may need to be established in advance and the content migrated in phases. To ensure practices are defensible, it is paramount that standard policies and practices are consistently applied to the release of collaboration content. Determining what is work product, internal correspondence, privileged communications/documents and drafts versus final versions is equally important.

DATA PRIVACY CONSIDERATIONS

Data Subject Access Rights (DSARs) relating to GDPR and other data privacy regulations need to be considered as they continue to emerge and evolve. At a minimum, the firm needs to be prepared to respond to a data subject's request for access, correction, erasure and portability of their personal information if the firm is holding such data. The firm should consult with their counsel to develop standards so they can consistently respond to such requests should they be made.

[2] Different collaboration tools have different messaging features and use different terminology to describe them. By "chats" or "instant messages," we mean messages exchanged between individuals on a more ad-hoc basis, as opposed to "posts" or "conversations" which are associated with and viewable by larger teams. The retention policies applied to these two different types of messaging may be different.

USE EXISTING TECHNOLOGY

The use of eDiscovery tools for review will likely become more critical as the volume and formats multiply. Some collaboration tools have inherent capabilities, such as Microsoft 365 eDiscovery, that allow legal holds in place to review content within the source collaboration environment. Continuous legal holds present other challenges potentially requiring a distinct strategy. But a word of caution: these capabilities are still maturing. Firms are also learning that using internal eDiscovery tools can be fraught with challenges. For example, unlike email formats, cloud collaboration content may not provide needed metadata, paths or threads because the content can be fragmented or sprawled. In many cases, the infrastructure was not designed for eDiscovery approaches. The option to export the content and sequester it elsewhere will be used for some time. Capabilities to migrate the content from one organization or tenant to another are emerging, with most being available only with direct vendor support. The use of migration tools automates the arduous process of exporting content from the source system, recreating access permissions and reimporting.

LEVERAGE EXISTING POLICIES AND PROCEDURES

Conversely, once the format and method of portability are established with stakeholders, the onboarding and importing format should be relatively straightforward, but likewise should follow standard policies and practices such as identifying and demarcating data received from prior counsel. Firms should update their IG Policy and related retention schedule to reflect how information contained within the collaboration site is to be managed. They should also have established practices on how long they retain content once exported or imported. Some firms inform clients that content will not be retained while others may retain content following the existing document retention schedules *[see Disposition of Content section]*.

CONCLUSION

Adoption of a collaboration solution at the firm brings new processes and technologies, but many of these are repackaged combinations of existing content management solutions. When considering data portability, look to your existing processes, procedures and technologies. Identify the content that needs to be captured and transferred then work with your internal resources to develop an appropriate strategy. Odds are that your existing processes, with a bit of ingenuity and tweaking, can provide the tools you need.

DISPOSITION

In an effective IG program, the concept of disposition should be both media and repository-neutral. Therefore, content created and utilized in collaboration spaces should be subject to the same disposition policy and procedure considerations, such as content ownership, location, rules and requirements, as other "official" content (e.g, content in the DMS). To this end, many firms choose to utilize the DMS as a tool in their collaboration space disposition workflow (e.g., at the close of a matter, move the content to the DMS) allowing them to follow established retention processes. See the Synching with DMS section.

CONTENT OWNERSHIP

When applying policy and carrying out the procedures associated with disposition, identification of ownership or custodianship is an important early step. It is well-established, but bears repeating, that clients ultimately "own" the bulk of law firm client records. Consequently, the responsible or otherwise designated attorney on a given matter who is often thought of as owning client records is better characterized as a custodian. The exercise of identifying custodianship for a given collaboration space may be as simple as extending this same methodology. This, however, may assume that collaboration spaces are matter-centric. Thus, the guidance around the structure and governance of collaboration spaces is a precursor to making decisions on disposition.

CONTENT LOCATION

Further considerations depend on whether the collaboration space is entirely internal or client-facing. Collaboration spaces that are entirely internal to the firm would seem to be best governed with the extension of the existing methodology discussed above, i.e., custodian attorneys are governed by the same ethical obligations to their clients as they are with any other hard copy or electronic records.

When external parties come into play, policies and roles need to be agreed upon at the outset. Clients may have retention and disposition policies that overlap or even conflict with the firm. Given the well-established precedent of client ownership of records, deference to clients' policies is likely appropriate. However, attorneys are still obligated to ensure that any such policies meet these stated ethical duties. Processes could be established to ensure that attorneys maintain copies of all documents and work product where additional retention requirements fall on the attorney and firm.

ADDITIONAL CONSIDERATIONS

The nature of a collaboration solution brings together several distinct content repositories that need to be addressed as part of the disposition strategy. Solutions like Teams and Slack include chats and conversations as well as document repositories. Each of these may have distinct retention and disposition requirements depending on the firm's existing policies. It is common to apply a shorter retention/disposition period on chats and conversations than to the underlying data, which may be subject to more specific retention periods under the firm's record policy.

In addition to the typical collaboration content that is subject to the firm's retention policies, in many instances the collaboration tool provides access to and even incorporates additional solutions utilized by attorneys through the tool. Examples of these include Teams and the availability of solutions like OneNote and Planner, both of which can be tied to the underlying Teams provisioning and structure. Unlike the standard retention and disposition policies that are applied at the Team level, these "additional" solutions typically require careful consideration when dealing with the disposition or end of life of a collaboration space. Additional consideration must be given to these solutions and the information stored within them. Often separate policies and procedures need to be developed to deal with these areas (e.g., what to do with OneNote and Planner content when a Team is being retired/deleted).

CONCLUSION

Just as DMS documents require defensible deletion procedures and hard copy records require secure destruction procedures, collaboration spaces require their analogous procedures to both decommission the space itself and ultimately dispose of the content held therein. Additionally, any considerations given to DMS disposition, such as Knowledge Management retention, regulatory compliance and client requirements, must be equally applied here.

EPILOGUE

As you've read through the various topics in this paper you likely detected a recurring theme… the tenets of good governance are applicable across all platforms in any software ecosystem. Collaboration platforms bring a level of ease of use that most users find appealing. The tools are, by and large, intuitive and do not typically require a high level of training to use. The issue for governance professionals is that they open the door to a vast array of potential data that firms must consider. Firms should make sure they have secured the fields with strong fences before they let the horses out of the barn.

IRON
MOUNTAIN®

800.899.IRON | IRONMOUNTAIN.COM

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.

USLGL-RPT-040122A