The Legal Intelligencer

Best Practices: Using Information Governance in the Discovery Process

We turn now to one of the most practical and rational ways an organization can impose reasonableness on the discovery process—Information Governance. Information Governance is a broad practice that determines the manner and means of organizing and managing an organization's information in the ordinary course of business.

By Tess Blair, Tara Lawler and William Childress | December 28, 2021 at 1:13 PM

(l-r) Tess Blair, Tara Lawler, and William Childress, of Morgan, Lewis & Bockius.

In our last article we reminded readers that Federal Rule of Civil Procedure (FRCP 1) is the lodestar for eData lawyers, that directs parties and courts to use the rules to "secure the just, speedy and inexpensive determination of every action and proceeding." FRCP 1 does not simply suggest that we endeavor to be rational and practical during discovery, it demands it. We proposed to use our next series of articles as a refresher on the fundamentals of discovery and the importance of reasonableness that should guide practitioners and inform best practices in every aspect of a discovery, and Information Governance (or IG) practice. In that first article, we reviewed the fundamentals of data preservation for discovery and covered some legal-hold best practices.

We turn now to one of the most practical and rational ways an organization can impose reasonableness on the discovery process—Information Governance. Information Governance is a broad practice that determines the manner and means of organizing and managing an organization's information in the ordinary course of business. Our IG practice, for example, assists clients in the development of policies and practices for every stage of the information life cycle

and advises those clients on a wide array of legal issues and risks that arise at each stage. Information Governance covers information from creation through disposition, with information security, privacy, acceptable use, retention and discovery sandwiched in between. Investment in good IG yields many benefits, including enhancing an organization's ability to secure and control its information; improving search, retrieval, use, and leverage of information; and reducing the proliferation of junk data that creates corrosive information noise throughout the business. For our purposes it also impacts future e-discovery obligations in a way no other investment can by delivering defensibility, efficiency, and command of an organization's data landscape that leads to far more favorable outcomes in the push/pull of discovery strategy.

A colleague recently shared the common complaint that some stakeholders in the discovery process expect companies to save all of their data for some hypothetical lawsuit in the future. Underlying this kind of mindset is the view that an organization's refusal to retain all of its data for long periods (or forever) is inherently suspicious. This view often leads to accusations of spoliation and the motion practice that ensues and is premised on a fundamental misunderstanding of Information Governance. Looking at everything through a prism of potential litigation can distract from the business goals of an organization and create unnecessary retention of noisy data. As the old saying goes, when the only tool you have is a hammer, everything is a nail. But, as we discussed in our article from last December, an eData lawyer's toolbox is full of tools (Dec. 29, 2020 article), and that is where IG comes in.

In the ordinary course of business, US organizations have broad latitude to manage information as they deem appropriate, informed by sound risk-mitigation strategies and practical business needs that are limited only by a patchwork of state and federal laws and regulations. Business need and regulatory obligations rarely last forever, however, and once those are gone, an organization should rationally endeavor to dispose of that data in a routine yet systematic way. Such disposition saves time and money, facilitates control and security, reduces risk, and—yes, as an added bonus—reduces the burden and cost of future discovery.

Disposition has to be defensible. As we all know, when an organization or person receives notice of an actual or reasonably anticipated lawsuit or investigation, all potentially relevant data in its possession, custody or control at that moment is subject to legal hold. It does not matter that the data is noise or that the organization should have deleted it long ago. If the organization has it, it must preserve it. The key to defensibility is a well-designed retention program, one that treats a legal hold as nothing more than an exception to an organization's routine management and disposition of data.

A concise retention policy and digestible retention schedule make up the backbone of a defensible IG program. A retention policy should clearly describe its purpose and goals and provide clear instructions on how to comply. In other words, it should explain what should be retained and what should not and why. The retention schedule should list the organization's business records by functional area (i.e., human resources (HR), finance, legal, operations, marketing, etc.) and the length of time the organization will keep each record. The schedule should also set forth the reason for the retention period (citation to a law, regulation, or business need). Because the schedule should reflect the organization, as well as that organization's obligations and culture, the most effective schedules are customized for and reflect the "language" of the organization. An off-the-shelf package rarely achieves a similar level of adoption and compliance.

Our team has a lot of experience with retention programs, both good and bad, and we have honed our approach to give clients a rational, practical way to implement a humane program that meets their IG goals. Gone are the days of thousand-page schedules and 20-click procedures to move an email to a designated system of record. Also gone? Full-time records-management teams manning warehouses of boxes. We now work in a self-service electronic business-information world, and governance has to both reflect and leverage that.

Here are five practical, rational things you will find in a Morgan Lewis & Bockius eData record-retention program:

- Records vs. Everything Else: We focus a lot on structuring the program to clearly define Records versus "Everything Else." Records are the business Records of the organization that it retains for legal, regulatory and business needs. All Records are listed on the retention schedule and will be retained as specified. If it is not listed on the schedule, it is not a Record. If it is not a Record, it is Everything Else. Everything Else, which we commonly call "nonrecords," junk, or "information of transitory value" if you are fancy, is noise and must be regularly purged regardless of location, format, love, neglect, hoarding habit or convenience. That is roughly 95% of email and at least half of the documents and other detritus scattered about on hard drives and file shares, in Box, Teams or Slack and so on. We encourage clients to set retention on Everything Else for the shortest practicable time, almost always two years maximum.
- Legal-Hold Exception: A legal hold is not the tail wagging the retention dog in our programs. While pending, a legal hold temporarily suspends the expiration of any information—whether Record or Everything Else (a very important point to repeat here is that legal holds apply to every potentially relevant bit of data in an organization's possession, custody, or control at the time the hold is triggered, whether a Record or not). We encourage clients to carefully scope their legal holds and to regularly review them to release information, custodians, and holds altogether at the soonest opportunity. Otherwise, legal holds become the barking retention dog.
- A Simple Schedule: Although we can and regularly do prepare detailed retention schedules with organized Record categories, definitions and descriptions, retention periods and citations, they become the roadmap for the legal or compliance group that is responsible for the retention program. For training and implementation, we prepare a shorter, simplified schedule—usually just a line or two per functional area but never more than a page. The simple schedule provides information owners with exactly the information that each needs to comply. The team gets the HR schedule that provides a single retention period for HR records (usually the longest common denominator), along with one or two outliers. That way, each owner only needs to remember two or three retention periods—not pages and pages (and pages) of irrelevant information—in order to comply.
- The Means to Comply: As we always tell our clients, drafting the retention policy and schedule is the easy part; compliance is hard. Planning ahead for the rollout and implementation of the program makes an acceptable level of compliance more attainable. Key elements of the rollout are timing, training, and the tools to comply. Timing is key because it is often wise to conduct a pilot or to incrementally stage the rollout rather than try to launch the program companywide all at once. Timing also means giving fair warning that the program is coming and making sure that it accommodates the requisite period of pitchfork wielding and teeth gnashing. The rollout of any updated or new retention program should always be accompanied by training, which should be short, sweet and

mandatory. Most important, rollout must provide everyone in the organization with the tools necessary to comply. If the program will require users to store Records in a document management system, users need access to the system and step-by-step instructions to move Records there. If the program requires Outlook retention folders, those folders should be auto-populated or instructions should be provided for users to make the folders. Finally, make sure that other policies such as access controls, auto-janitors or folder size limits do not undermine compliance.

- Consistency: We strongly urge clients to take special care to enforce the policy consistently and to conduct audits or purges regularly in the ordinary course of business. A policy that selectively targets some documents for destruction or is applied inconsistently or randomly can give rise to an inference that it has been used in bad faith to clean out "unhelpful" documents in advance of an anticipated litigation or investigation. This is why we often hear that a retention policy ignored is worse than no policy at all.

In our next installment of this series on e-discovery basics we will focus on the practice of analyzing and assessing the sources and locations of client data (some call it "data mapping") and preparing a discovery playbook for e-discovery readiness.

For those interested in a comprehensive discussion on the topic of Information Governance, the Morgan Lewis eData practice has just released the fourth edition of the "EData Deskbook." In its 10 chapters, the deskbook provides practical guidance for all lawyers and discovery managers responsible for litigation and IG. It includes tips and best practices for addressing some of the most challenging aspects of managing complex discovery across all stages of the Electronic Discovery Reference Model (EDRM).

Morgan, Lewis & Bockius partner Tess Blair is the founder and leader of the firm's eData practice. Partner Tara Lawler 's practice focuses on e-discovery, information management, and data privacy. Associate William Childress counsels clients on electronic discovery.