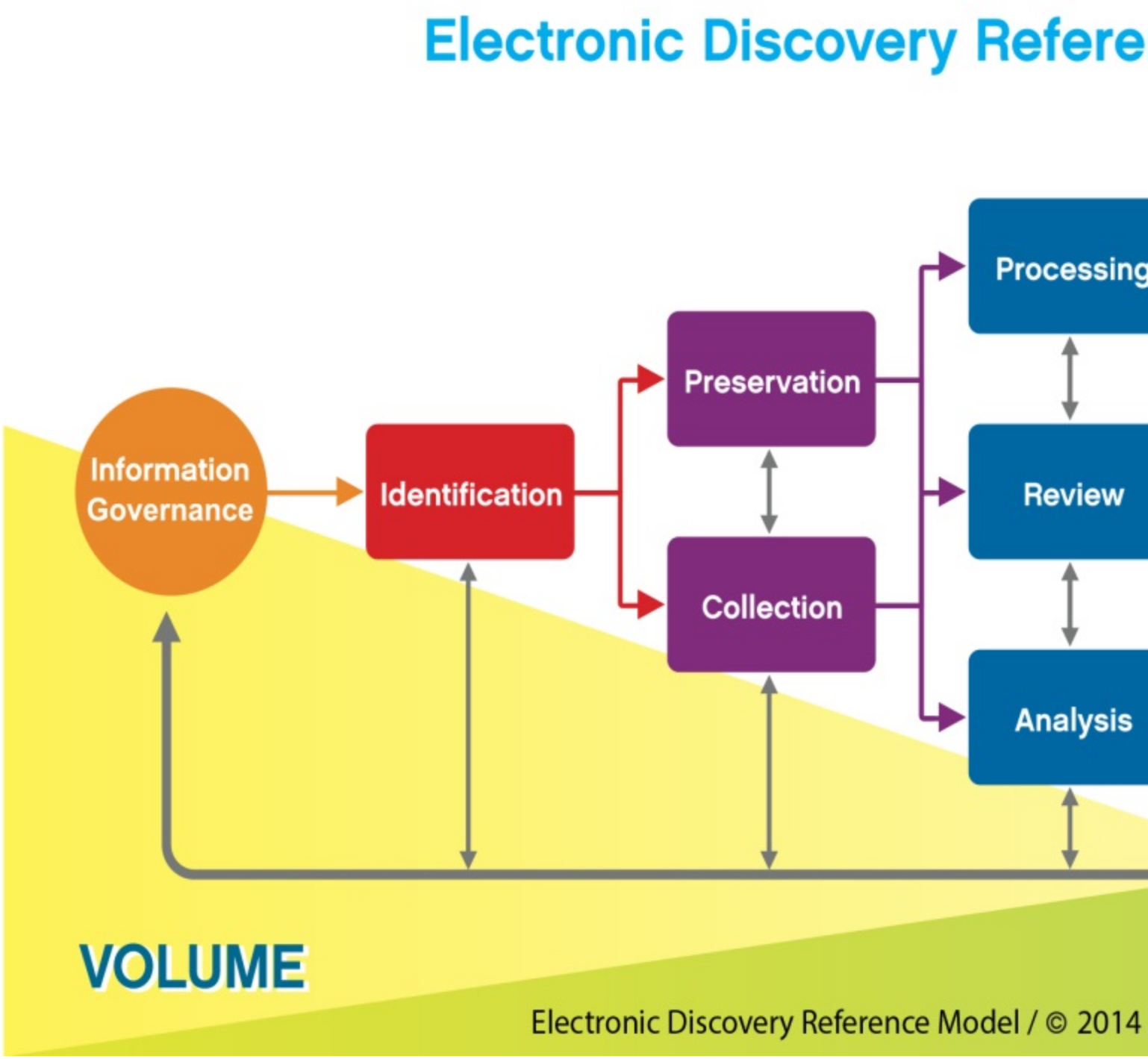
PUBLICATION

Electronic Discovery Preparedness Audit Handbook [Ober|Kaler]

September 23, 2016

While your organization may not regularly be involved in costly or complicated litigation, there are instances in which it may nonetheless be required to identify, collect, and produce documents most likely in the form of Electronically Stored Information (ESI). This need may arise as part of a direct or indirect government investigation into your organization. What is certain though is that once the need to produce ESI is established, the costs begin to mount almost immediately. Identifying which documents to produce, reviewing these documents for privilege and responsiveness, and ultimately producing the documents to the government takes time and money. Outside vendors that need to be brought in to assist in the process typically charge for all time spent discussing the approach to collecting data, as well as for the time to actually collect and process the data for production. The collection and processing charges are directly impacted by the volume of data, typically on a per-gigabyte basis. Given that just one request can lead to tens or even hundreds of thousands of dollars in response costs, it behooves all organizations to prepare for this eventuality.

This handbook will assist your organization in completing a full audit of your Electronic Discovery Readiness. It is broken into categories reflecting the various preliminary steps your organization should be proactively taking to ensure that it is prepared when a request to produce ESI is received.



Information Governance

The most efficient way your organization can reduce its exposure to unneeded risks and costs in the event it does need to produce ESI, is by ensuring that your organization only archives data for which there is a legitimate business need or legal requirement. Although it may be tempting to archive more ESI than your organization is required to, doing so not only makes it more difficult to locate potentially relevant data, but it may lead to greater production expenses. Further, having an investigating agency sifting through data that was needlessly produced as a result of not adhering to a Document Retention Protocol, may cause additional investigation inquiries that would otherwise not have been considered. This section will help your organization assess its approach to ESI storage and suggest ways to limit and focus the ESI it chooses to store.

1. Records Retention Schedule.

Your organization should create and maintain a fixed schedule for how often data is archived, where it is archived, when it is moved to long term storage, and when it is ultimately destroyed. A log or tracking index should be maintained to show the progression of data from archiving through destruction.

Evaluate Legal Requirements. Your legal team should determine what the legal requirements are in your industry in terms of how long your organization keeps certain categories of data. It is important to evaluate each potential category separately to ensure you are not storing and maintaining more data than required simply because another type of data requires a longer storage period.

Evaluate Business Necessity. Your organization should determine how long it actually needs to store emails, legacy files and systems, and other data so as not to fall into the easy trap of storing everything your organization generates. Just because your company can cheaply and easily archive data beyond the legal requirements or your business needs does not mean it is reasonable or advisable to do so. The more data your organization has, the more potential exposure to higher data collection costs, review costs and production costs.

2. Data Mapping

The larger your organization, the wider its data footprint. A data map is not only helpful in identifying sources of ESI as outlined in the Identification section below, but it ensures that your organization has an easily accessible picture of its data footprint. This can help streamline the way your organization manages its data and make it easier to identify opportunities for improved efficiency and cost savings both in the context of electronic discovery and more generally as to IT expenses.

3. Employee Education

Records Retention Policies should be clearly described and explained to all employees. Transparency in the process leads to improved compliance. Employees are far more likely to adhere to Records Retention Policies when they understand that the policy is not arbitrary, but rather, confers a substantial benefit to the organization and ultimately to the individual employee.

4. Create written policies and monitor compliance with the policies. It is important that all policies related to information governance (i.e. Records Retention Policies, Archiving Protocols, etc.) are in writing and distributed widely within your organization. Once a policy is in place, it is important to monitor compliance with that policy through regular audits. Periodic updating of the written policies should be done to ensure compliance with current legal requirements and business needs. Examples of other regular audits include:

Data age audits. Regularly check to see if data past a previously determined age is being stored contrary to policy (i.e. not due to a litigation hold or business exception).

Storage audits. Check regularly to ensure that all storage policies, including data destruction policies, are being followed. All storage should be easily identifiable and stored in a manner accessible using current technology.

Third party audits. Make sure to regularly check for changes to storage/backup policies of any third party vendors, including email, cloud storage, and patient records vendors. Ensure that all audits also include monitoring third parties for compliance with their stated policies.

Departing employee audits. When an employee prepares to leave your organization, ensure that their data is properly mapped and stored. This is of particular importance so that knowledge about their data does not depart with the employee.

5. Storing Data

Create and maintain a centralized location for short-term storage. This can be one centralized location within the entire organization or it can be within an individual business unit. This should be for data that is not needed on a regular basis, but for which there is an anticipated need to call.

Create and maintain a location for long term storage. This should be for data that will likely not need to be recalled, but which must be stored for legal/compliance reasons or business needs.

Monitor the form of all storage media and update as needed. Storing legacy data for which no hardware or software environment exists only leads to additional unwarranted scrutiny and greater processing costs. Obsolete systems which contain unneeded data should be avoided at all costs. If the data must be stored, it must be accessible.

6. Purging Data

Create a fixed schedule for when legacy data (no legal or business requirement for keeping it) can be safely destroyed.

Have your organization's legal department confirm how long your organization is obligated to store various types of data.

Check with department heads from each department within your organization to determine if any business reason exists to extend the retention period beyond the legal requirements.

Once these timeframes have been established, enforce them by deleting all data that age past the predetermined point. This data purge must be done regularly to ensure unneeded data is not being stored.

Identification

Even if your organization does not store extraneous data, it is still important to have a firm grasp on the nature of all stored ESI in your organization. It is essential to discuss ESI locations with the right people for each project in advance so that data collection can proceed in a targeted and focused way when the need arises.

7. Develop an Identification Team

The team should consist of corporate counsel, outside counsel, records management, IT personnel, HR personnel, and the heads of each department within your organization.

Ensure that at least one key stakeholder in each major project knows where archived data is stored to assist the team.

8. Establish universal policies and procedures for the storage and archiving of data and communicate these policies to all employees.

Create a data retention manual. This should build upon your organization's Information Governance Policies and assist all members of your organization in complying with those policies.

Provide technical support for your employees in managing their data in accordance with all relevant policies.

9. Data Map

Determine what computer systems are in use in the organization.

On Site. Determine what hardware, shared resources, servers, networked locations, email servers (including lists of users and storage locations), temporary storage (flash drives, etc.), long-term and backup storage are used to store ESI.

External. Determine what types of storage locations organization members use while travelling or while working outside of the office. Personal computers, tablets, phones, temporary storage, and anything else used for storing ESI should be included.

Third Parties. Determine what third party systems your organization uses to manage and/or store ESI. You should have a complete understanding of the ESI maintained by email, cloud storage, web hosting, and patient/customer records vendors, including their policies and procedures for data storage and backup.

Determine how or if these systems are connected. Assess in advance what the most centrally-accessible location to collect ESI would be should a collection be necessary. Oftentimes, simply crafting, implementing, and enforcing a backup schedule is sufficient.

10. Document any and all alterations to the ways or locations in which ESI is stored.

Preservation

Your organization can be exposed to great risk should it destroy information that was legally required to be preserved. It is essential to educate all members of your organization concerning the importance of adhering to preservation notices and to ensure that all such notices are sent out promptly to prevent inadvertent destruction of ESI. To that end, it is crucial that the technical ability to create and effectively distribute litigation holds be in place prior to receiving any ESI requests.

11. Create and use a standardized litigation hold form to let all relevant individuals know that a litigation hold has been made and that all relevant data should be preserved per the Record Retention and Archiving Policies.

Ensure that a proper litigation hold has been distributed to all the appropriate parties.

Ensure that all ESI sources (email servers, personal computers, backup tapes, etc.) have been included in the litigation hold.

Follow up to ensure that the litigation hold has been put in place. Compliance monitoring is a necessary and required part of the preservation process.

12. Create a method of documenting and tracking the preservation of relevant data and noting where exceptions are made to your organization's records retention and archiving policies.

13. Mitigate risks by developing a comprehensive preservation plan where the process is enforceable, defensible, and repeatable.
14. Understand the technical capabilities of your organization's IT department as well as all third-party vendors who host data.

What capabilities does your organization's email system have to implement a litigation hold? Is a third party needed to help execute the litigation hold and ultimate archiving of that data?

What capabilities does your file server have to prevent deletion of data flagged for a litigation hold?

What functionality is included in third-party software employed by your organization to implement a litigation hold?

Collection

After following the steps outlined above, collecting relevant ESI can be a relatively straightforward process. If your organization has properly put into place policies that address retaining and archiving of data, collecting and producing ESI will be a much more efficient and cost effective undertaking.

15. Use your data map to help your organization create data management policies with the potential need for a data collection in mind. Proactively consider the collection process appropriate for the location and nature of the relevant ESI. Make sure that this process is enforceable, defensible, and repeatable. Understand the capabilities and limitations of each software environment used by your organization to collect data. Consider bringing in outside experts to ensure proper collection and data integrity.

Use your organization's experts and outside counsel earlier on in the process to ensure that collections are being done correctly and that a process is in place to track the data from collection through production.

If you have any questions about this handbook or if you would like to consult with an eDiscovery attorney regarding your organization's policies and procedures, please contact Baker Donelson.