

DOCSVAULT WhitePaper

Concise Guide to E-discovery

Contents

- i. Overview
- ii. Importance of e-discovery
- iii. How to prepare for e-discovery?
- iv. Key processes & issues
- v. The next step
- vi. Conclusion

Overview

E-discovery is the process of identifying, preserving, collecting, reviewing, analyzing and producing case relevant information during civil or criminal legal actions. The matter presented during e-discovery is useful in pre-trial motions as well as in the trial itself. Information sought during e-discovery can include electronic documents, testimony and other information that may be considered necessary by the court.

Electronic content is growing rapidly as seen in the following facts.

- ✓ According to University of California 93% of all information today is created in electronic format
- ✓ The American Records Management Association says more than 90% of records created today are electronic
- ✓ More than 70% of electronic information is never printed

According to a study by IBM 15 petabytes of data is created every single day.



E-discovery is an extension of discovery, “the compulsory disclosure of pertinent facts or documents to the opposing party in a civil action, usually before a trial begins.”

It is a well-established process pertaining to the electronic content including email communication, instant messages, word files, spreadsheets, presentations, invoices, contracts, social networking content and all other electronic content created in an organization. Data for e-discovery can be stored in desktop computers, laptops, smart phones, backup tapes, servers and even employees’ personal computers.

Preparing for e-discovery is not only useful for litigation purposes, it also helps in a number of ways including managing and avoiding employee misconduct and legal actions, complying with regulatory obligations, preserving intellectual property, knowledge and other data, helping in storage management and avoiding embarrassing data loss or theft.

Organizations can prepare for e-discovery appropriately if they understand the importance of e-discovery, gain insight into key issues and relevant regulations and create an infallible strategy with the help of technology so that the data is managed, preserved and produced properly.

Why is preparing for e-discovery important?

Every organization is under obligation by law to retain and dispose its data carefully so that they can respond to e-discovery requests quickly without any scope of human error; understand which data can be accessed and which cannot be; and discover the growing variety of content.

Benefits of E-discovery

There are many benefits to preparing for e-discovery; some of them include:

Prepare for e-discovery request during litigation

Early preparedness for e-discovery can help an organization to perform early case assessment and understand its legal position. It can also result in discovering some proofs to gain advantage over opposition. This can reduce legal fees and other expenses.

Reduces risk of lawsuits on the whole

If a strict policy of e-discovery is followed in an organization, it can monitor employee behavior for actionable statements or activities, and reform and enforce corporate policies quickly.

Saves time and money

Preparing for e-discovery can save time and efforts of staff and legal counsel during e-discovery request, resulting in prompt response. It can also reduce costs like legal counsel expenses, email and records management software, storage and provide a number of other savings.

Saves from unfavorable legal judgments, fines and bad press

Good e-discovery capabilities allow organizations to make prompt and accurate decisions, as they are equipped with better information. This increases the chances of favorable judgment during trial, reduces legal costs and decreases time required to resume normal business operations. It also saves from fines, damage to goodwill and public relations from negative press and other more dramatic outcomes.

Major Benefits

- Prepares for civil or criminal litigation
- Reduces risk of lawsuits altogether
- Saves time and money
- Saves from unfavorable legal judgments, fines and bad press



E-discovery Process

E-discovery process reduces risk through improved regulatory and corporate compliance. Preparing for e-discovery involves the following steps:

- I. Identification
- II. Classification
- III. Analysis / Review
- IV. Preservation
- V. Presentation

It is important for all organizations to train their employees to preserve all electronic files, communication and other electronic data. Judges have little or no patience for lawyers or clients that are not prepared for e-discovery request or don't understand it.

DMS for E-discovery?

Document management system allows organizations to prepare for e-discovery with the help of tools like document profiling or metadata preservation, version control, audit trail, security and document retention.

E-discovery Steps

- i. Prior to litigation
- ii. Reasonable Anticipation of Litigation or Known Litigation
- iii. Production
- iv. Post-litigation

How to Prepare for E-discovery?

Prior to litigation

- ✓ Train staff to recognize electronic data such as files and communication for “potential litigation”
- ✓ Form an e-discovery records policy with stakeholders including IT, HR, Legal and regional managers
 - Understand the knowhow of document management and retention plan
 - Understand processes that might affect collection, tampering, preservation, and deletion of data
 - Adopt software system to ensure smooth document processing
 - Create a data map to ascertain where data is stored and check its consistency to see whether it is accessible or not; classify data such that only authorized staff can access it
- ✓ Familiarize staff with the document management and retention plan
- ✓ Perform routine computer and IT checks to ensure you can take advantage of the Safe Harbor rule
- ✓ Standardize processes of repeatable operations like document collection, review, privacy and security issues, etc.

Reasonable Anticipation of Litigation or Known Litigation

- ✓ Implement your litigation hold policy
- ✓ Identify imminent spoliation concerns and take immediate action
- ✓ Determine scope of discovery, including file types, 3rd party data sources, no. of custodians, accessibility/inaccessibility of data, metadata, backup media and date ranges
- ✓ Send written notices to involved personnel
- ✓ Follow up orally or in e-mail at least quarterly with personnel
- ✓ Prepare for your meet with opposing counsel after conferring with IT personnel
- ✓ Determine how the court prefers to handle e-discovery issues, i.e. local rules or standing orders
- ✓ Begin the budgeting process
 - Determine scope, devices, accessibility of data, number of custodians and volume of data
 - Determine reasonableness and proportionality of what the discovery should cost in terms of the exposure of the case
- ✓ Implement collection of data – paper and electronic
 - Determine who will collect the data, i.e., staff, custodians, attorneys, and/or IT personnel
- ✓ Choose & Process Data
 - Scan and code paper documents
- ✓ Review Data
 - Define standardized review process for Privacy, Privilege, Audit log, etc

Production

- ✓ Produce data in the form agreed upon. If no agreement, give opposing counsel notice of the form you intend to use for production. Give opposing counsel time to request an alternate form

Post litigation

- ✓ Notify custodians that litigation has ended and the hold is removed. Instruct them to follow normal document retention procedures with regard to the data held. Notify them that some of the data may be pertinent to other legal holds and should be maintained per those hold instructions

Federal Rules for E-discovery

According to the amendments to the FRCP that went into effect on December 1, 2006, organizations must manage their data in such a way that this data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings. The key issues that brought about these amendments are:

- ✓ Electronic data is normally stored in a greater volume than hard copy documents
- ✓ Electronic data is dynamic and can be easily modified or spoiled
- ✓ Electronic data may become incomprehensible when separated from the systems that created it
- ✓ Electronic data contains non-apparent information, or metadata, that describes the context of the information and provides other useful and important information

- **Identification**

The main issue during litigation is identifying relevant data that is to be presented. DMS features like document metadata and other folder sorting features can help ease the process of understanding the universe of information required and respond to e-discovery requests better.

- **Preservation**

This critical step needs to be taken to ensure that data is protected from spoliation and tampering. If spoliation occurs, the consequences can be expensive. DMS offers fine-grained security to protect data from spoliation.

- **Collection**

During this phase, all relevant ESI is collected from the various sources that contain it, including emails, backup tapes, file servers, desktops, laptops, employees' home computers and other sources. If a strict record management policy is followed with the help of software system, this step becomes less expensive and time consuming.

- **Processing**

Collected data should also be processed into a) relevant data and b) data not relevant during litigation. Shared repository, review and comment process can make this step easier.

- **Analysis**

This phase involves different kind of activities such as determining exactly what the data means in the context of litigation, developing summaries of relevant information, determining the key issues on which to focus, etc.

- **Production**

The production of data involves bringing the relevant data to any parties or systems that are concerned. It also includes the activities focused on delivering data in the appropriate form(s), including DVDs, CD-ROMs, paper, etc.

- **Presentation**

It is a recognized issue that some electronic data becomes incomprehensible outside the system where it was created. It is important to adopt technological software that does not change the format of data at any stage of document process.

Key Steps & Issues

- Identifying relevant data
- Protecting data from spoliation
- Analyzing data prior to litigation
- Producing and presenting data

DMS must have tools to enhance productivity, management, security and collaboration.



What should you do next?

While it may seem from the above information that it is easy to prepare for e-discovery, it is important to understand that putting this information in action rather than leaving it as a theoretical exercise is easier said than done. Don't ignore this exercise thinking it won't be needed in your organization and take the next step.

What e-discovery means for a particular organization?

The first step is to determine in which way e-discovery is important to a business or organization. Apart from the law and regulatory compliance, there are many other factors such as potential litigation or audits that make it important for organizations to prepare for e-discovery. Since every organization, its policies, business processes and technologies are different, the way it prepares for e-discovery is different too. It is important to consider industry standards, budget and policy to justify e-discovery in future before forming any policy.

How to form a data retention and deletion policy?

Every organization must set data retention and deletion schedules for all its data in order to meet current or potential e-discovery or other requests. Most organizations out of fear of deleting important data often retain more data than required. This can lead to higher expenses in terms of storage and longer time spend in analyzing, reviewing and presenting in time of e-discovery request. Legal counsel can prove to be helpful in forming a data retention and deletion policy.

What e-discovery tools are needed?

The next step is to adopt tools that enable organizations to prepare for e-discovery. These technological tools help by making data more accessible and easily reviewable during the early case cycle. Tools like document management system can help classify data since the time it is created with the help of metadata properties until the time of discovery through faster search feature.

How to implement legal hold capability?

If a legal action is expected or once it is in progress, it is necessary that an organization immediately initiate identification and preservation of all relevant data, such as all emails sent from staff to concerned individuals and all data concerning the litigation. If properly prepared for e-discovery, organizations can right away place a hold on data when requested by a court or regulator, or on the advice of legal counsel, and retain it for as long as necessary. If an organization is not properly able to place a hold on data when required, it can face a variety of negative outcomes, such as legal fines, bad publicity and loss of face. Docsvault document management software provides record management features such as data retention and deletion. You can even put data on hold during anticipated or ongoing litigation with the help of this feature.

Questions to Ask

- What e-discovery means for an organization?
- How to set data retention and deletion schedule?
- What e-discovery tools are needed?
- How to implement legal hold capability?

Conclusion

It is no longer optional but mandatory to be prepared for e-discovery. This must be done to proactively manage legal actions, regulatory audits and other such activities and respond to them quickly. An organization has a lot of obligations in order to prepare for e-discovery, including becoming completely aware of all the past, current and potential information and deletion obligations; effectively managing and retaining documents and data; implementing software technology that can ease processes such as preservation, deletion, production and retention; be prepared for litigation and take steps to minimize the risk of non-compliance with e-discovery obligations. Docsvault helps organizations to comply with e-discovery obligations with the help of features such as comprehensive and full text search, document profiling, email integration, version control and audit trail that ease e-discovery processes such as preservation, analysis, production and presentation.

Docsvault

Mailing Address

For mail correspondence, please use:

Easy Data Access
501 Scarborough Dr.
Egg Harbor Township, NJ 08234
USA

Get in touch

Monday to Friday
10:00 a.m. – 6:00 p.m. (EST)

Toll Free USA: (888) 819 3035
International: +1 (732) 960 3330
Fax: (888) 819 5965

E-mail us on:

Sales@Docsvault.com