

Electronic Discovery

By creating a real-time archive for all structured and unstructured data, EDMT® Server enables firms to efficiently and quickly comply with federal and state [electronic discovery rules](#), avoid discovery [sanctions](#), and implement [automated document retention policies](#) and [litigation holds](#).

EDMT® Server and Electronic Discovery

EDMT® Server enables you to comply with e-discovery requirements by:

- (i) creating a single, centralized repository for the entire firm that is accessible within a single search. Having only one place to search for all Electronically Stored Information (“ESI”) means you can reduce or eliminate the need to search for email and documents on multiple (perhaps hundreds) of laptop computers, and thereby quickly comply with FRCP 26(a)(1), which requires early identification of all ESI data;
- (ii) implementing automatic document retention and deletion policies by a category of documents, such as “all emails”, or “all client emails for Matter 001-001”. Deletion is automatic at the expiry of the retention period, thereby saving disk space and limiting exposure to legal risk, and
- (iii) when a “litigation hold” duty is triggered, instantaneously searching all structured and unstructured data for the entire firm, from a single interface, and applying bulk “hold” for all relevant data.

E-Discovery Rules

Since December 2006, the Federal Rules of Civil Procedure have established specific rules regarding the production of ESI. Since then, courts have issued a significant body of case law interpreting and applying these rules – sometimes with sweeping and serious results. At their core, the federal rules (and their state counterparts) require potential litigants to have a clear and comprehensive understanding of their ESI so that they can search and produce such ESI if necessary as part of the litigation process. If a litigant does not know where its ESI is stored, and has no consistent document retention policies – then the places where a litigant may be required to look for responsive ESI are potentially unlimited. This, in turn, adds unnecessary expense and months or years to comply with discovery requirements that require fast production times.

FRCP 26(a)(1) - *Locations of ESI*. This rule requires litigants to provide information to the opposing party, generally within 90 days of a complaint being filed, about the category and location of “all ...electronically stored information that the disclosing party has in its possession, custody or control and may use to support its claims or defenses”.

FRCP 37(e) – *Document Retention Safe Harbor*. This rule provides a “safe-harbor” for ESI that cannot be produced because it was destroyed as part of a “routine, good-faith operation of an electronic

information system". This means that a party cannot be sanctioned for a failure to produce ESI that has been destroyed as part of a routine document retention plan.

Sanctions

FRCP 37(b) – *Sanctions*. The first step in obtaining sanctions is to seek a motion compelling the discovery sought. For instance, a party may file a motion to compel where an opposing party has failed to make the initial disclosures under FRCP 26(a)(1). If that party further fails to comply with the motion to compel, the court may order sanctions, that may include:

- monetary sanctions,
- taking the facts at issue in the discovery dispute to be established,
- striking pleadings, and
- rendering default judgment against the disobedient party.

Automated Document Retention Policies and Records Management

The first step in establishing an e-discovery strategy is to identify what kinds of business records exist in a firm's business. In the case of a private law practice, a firm would have contracts (like engagement letters), correspondence with clients, opposing counsel and experts, filings, and work product (like a contract, or a complaint, prepared on behalf of a client). There would also be invoices, billing records (like expenses), phone records, etc...

EDMT® Server enables each firm and/or user to automatically categorize each item of ESI (through automatic EDMT™ Server's auto-filing technology), and to apply specific retention policies to each category of data. For instance, the default rule in EDMT® Server is that an email/ document will be held for at least three years from the date of creation, or ingestion, in EDMT® Server. Individual files of special interest or value, like an important contract, can be maintained indefinitely. After the retention period has expired, all ESI items subject to the policy will be automatically deleted from the system, unless there is a "litigation hold" (described further below).

One of the information technology, and legal, benefits associated with EDMT® Server is the ability to have retention periods automatically created, and have expired materials automatically deleted. This creates less data to store (on servers and on your local machine) which reduces storage costs, clutter and exposure to legal liability.

Litigation Holds and Centralized Search

A litigant is under a legal duty to preserve all information that may be relevant to a dispute as soon as it is "reasonably foreseeable" that litigation is likely. Once this duty is triggered, a litigant must prevent the destruction of possibly relevant material; this action is called a "litigation hold". In the case of ESI, this means, among other things, suspending an automated document retention policy. Assume, for example, that a firm implements a 1 year retention policy after an engagement has ended, and that the client raises the threat of litigation on the 350th day following closing of the Matter. With a click of a button, EDMT® Server enables the firm to suspend its ordinary document retention policy, and preserve all emails for that Matter that otherwise would have been automatically deleted with 10 days of the litigation hold duty triggering.