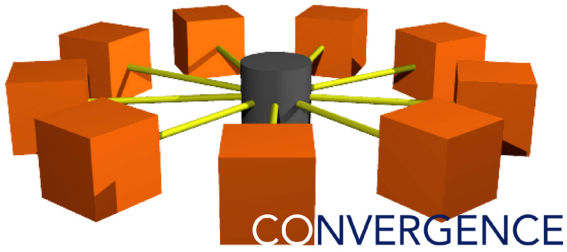
JMBM | Jeffer Mangels Butler & Marmaro LLP

Discovery Technology Group™
White Paper Series
May 2006

DOCUMENT RETENTION POLICIES



An effective document retention policy is one of the most important strategies a large corporation can develop to limit liability and expense and to effectively advance its business goals. In today's business environment, a company must consider three different goals related to its records:

1. the need to efficiently create and use documents in day-to-day business,
2. the need to retain records for regulatory compliance, and
3. the need to manage information in a manner that will allow it to comply with potential litigation demands at a minimum of cost and work disruption.

Unfortunately, it often appears that these three goals are opposing. Yet, at the same time, a document retention policy that fails to account for all three can be costly, unwieldy, and potentially catastrophic.

On the other hand, a document retention policy that represents a successful convergence of these needs can greatly improve a company's productivity, ease the burdens of regulatory compliance, and minimize litigation costs.

The following represents a checklist of key elements that every document retention policy should address and will provide us with a construct for examining how to create and maintain a successful document retention policy.

Compliance with Statutes, Regulations and Requirements

Does your company's retention plan ensure compliance with applicable legal requirements?

A few key statutes, regulations and requirements (depending on industry) to consider:

- SOX
- PTO
- Fair Labor Standards Act

- EPA
- Health Insurance and Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act of 1999
- OSHA
- IRS
- Consumer Product Safety Act
- ERISA
- Contractual restrictions
- State laws (many have different standards governing document retention)
- International (if applicable)
- Privacy requirements (must address both state and federal law)

Checklist For Document Retention Policies

£ Does your retention plan define how, where and how long to store both paper and electronic records, specifying retention periods for specific categories of records?

£ Does your retention plan address all forms of electronic data (e.g, e-mail, IM, wordprocessing, spreadsheets, digital copiers/printers, voicemail)?

£ Does your retention plan specify how records are to be destroyed when their retention period has expired?

£ Is the destruction of records specified in your plan automated or are individual employees responsible?

£ Does your retention plan break down requirements by department (or working groups)?

£ Does your retention plan detail the circumstances under which the policy should be suspended, such as when a lawsuit is anticipated?

£ Does your retention plan specify the individuals responsible for enforcing, monitoring and updating the policy?

£ Does your retention plan specify penalties for noncompliance?

£ Does your retention plan describe how to organize and catalog stored records, so that they can be easily recovered?

£ Are all employees required to review and sign your retention plan?

£ Does your retention plan establish a records compliance task force that meets regularly, i.e., employees are responsible for implementation and ensuring compliance with the plan?

£ Does your retention plan specify an IT employee that will be designated as the "person most knowledgeable" on the retention plan, implementation and compliance?

£ Does your retention plan specify that it will be routinely audited? Does the company ensure that the results of such audits are privileged, even though the plan itself is discoverable?

£ Does the retention plan specify that it will be routinely updated?

_____

£ Does the company plan to take steps to modify the document retention plan prior to the effective date of the New Federal Rules of Civil Procedure?

If so, are you considering the following:

- £ a) Audit and review of the plan to comply with the Rules?
- £ b) Designation of all e-data maintained by the company as either readily accessible or not readily accessible?
- £ c) Review of legacy data maintained by the company?
- £ d) Review of archival data maintained by the company?
- £ e) Joint review of system architecture by legal department and IT department to prepare for new early meeting of counsel requirements?
- £ f) Protocols for producing electronic data in a reasonably useable format?
- £ g) A litigation hold procedure and a litigation response team for preserving e-data and metadata?
- £ h) Isolating and protecting privileged electronic information from disclosure by indexing and storing before litigation arises?

£ i) Policy statements and procedures to ensure that any loss of e-data are "routine" and in "good faith," to fall within the safe harbor provision in the Rules to avoid sanctions for destroying electronically stored information?

JMBM's Discovery Technology Group™ counsels clients on preparing ahead of time to respond to requests for electronic information in litigation; complying on an ongoing basis with regulations requiring records retention; and having an IT system that supports these goals while still providing efficient and cost-effective infrastructure for day to day company operations.

Contacts:

Stanley M. Gibson
310.201.3548 • mailto:SGibson@jmbm.com

Dan P. Sedor
310.201.3554 • mailto:DSedor@jmbm.com

Michael A. Gold
310.201.3529 • mailto:MGold@jmbm.com

Robert E. Braun
310.785.5331 • mailto:RBraun@jmbm.com