MURPHY, HESSE, TOOMEY & LEHANE, LLP
Attorneys At Law

Corporate CLIENT ADVISORY ALERT

February 2007

CLIENT ALERT
Electronic Document Management Policy

If you do not already have an electronic document management policy, you should consider implementing a formal policy regarding the retention and destruction of electronic information in order to minimize costly discovery requests and to avoid possible court sanctions for the improper destruction of electronic documents. If you have an existing electronic document management policy it should be reviewed to ensure it is in compliance with recent legal decisions and guidelines.

Major changes to the Federal Rules of Civil Procedure became effective December 1, 2006, making it clear that the courts now explicitly recognize that the discovery of electronic information will be a key element in many legal actions.[1] Now more than ever, it is important for businesses to have proper procedures and practices in place to handle their electronic files. The retention of electronic information is a balancing act. While it is necessary to save some electronically stored information to comply with regulatory and litigation requirements, maintaining too many electronic records greatly increases the costs of e-discovery and can cause other problems such as decreasing business efficiency.

I. Creating a Document Management Policy

There is no single standard or model that must be followed in creating a document management policy and your policy should be tailored to your particular business needs, operations, IT infrastructure and regulatory and legal responsibilities. When creating a document management system, it is important to involve not only key management personnel but also IT staff and legal counsel. You do not need to retain all of the information ever generated or received, and you should destroy information that is no longer needed as long as the destruction is done in a systematic way.

---

[1] *See e.g.* FED. R. CIV. P. 16, 26, 33, 34, 37 and 45, as well as Federal Form 35.

It is essential, however, that your document management policy include a procedure for the suspension of the ordinary destruction of data when there is reasonably foreseeable litigation, government investigations or audits.[2]

Your document management policy should address the various places electronic files may be stored well in advance of litigation. There may be documents hiding on old hard drives, lurking on laptops, files on employees' home computers, information on thumb drives, servers on and off site, back up tapes, palm pilots, blackberries, and electronic phone systems. Also, as most of you know, when electronic documents are deleted, they usually do not completely disappear. A forensic expert can likely recover most documents, or information about the document deleted, from a hard drive.

The changes to the Federal Rules of Civil Procedure now explicitly reference electronically stored information in the rules governing pretrial conferences, automatic disclosures, discussions between parties, interrogatories, production of documents, sanctions and subpoenas. One of the biggest changes to the Federal Rules is that the federal courts will now require the exchange of electronic discovery during the first few weeks of litigation.[3] If a party does not know exactly where and how all of their electronic information is stored, it may be very difficult and expensive to find such information under the time pressure of discovery deadlines. Further, if an organization is not prepared for this immediate production of documents, mistakes such as producing privileged or attorney work product materials could occur. Therefore, it is prudent and certainly more cost-effective to set up a document management system in the regular course of business, as opposed to doing it in an emergency situation.

II. Records that must be retained - Litigation Holds

You should maintain records for business reasons, regulatory requirements and "legal holds". Our courts now mandate that when litigation is reasonably anticipated or pending, a hold procedure designed to ensure that relevant records are not lost or destroyed must be implemented. Therefore, if you are sued or even if there is a reasonable basis to anticipate litigation, legal counsel should be consulted immediately. It is important to discuss with your counsel what circumstances constitute anticipated litigation because if relevant documents or information are deleted, altered or destroyed during this time period you could be subject to court sanctions.

Your policy should also address how "metadata" is stored because it may be discoverable.[4]

---

[2] *Id.*

[3] FED. R. CIV. P. 26(a), the Initial Discovery Rule, now requires a party to provide, "a copy of, or a description by category and location of, all documents, electronically stored information . . . that the disclosing party may use to support its claims or defenses." Under the FED. R. CIV. P. 16(b), the Scheduling and Planning Rule, a judge may include "provisions for disclosure or discovery of electronically stored information" in a scheduling order.

[4] *See* Committee Notes to Amended FED. R. CIV. P. 26.

Metadata is information embedded within the digital framework of an electronic file including who emails are to and from, a file's name, location, format, size, when and by whom it was created, modified or last accessed. Because metadata is discoverable, you need to know what metadata is and how and when to preserve it to avoid potential court sanctions.

III. Court Imposed Sanctions for Destruction of Relevant Information

Spoliation is the legal term used for the "destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[5] Our courts are now permitted to issue a wide range of sanctions for spoliation. If a court finds fault in an organization's document retention practices they may order the organization to pay the costs of additional discovery such as the re-deposition of key witnesses, or the court could order the organization to pay all reasonable expenses incurred by the adverse party, including attorney's fees.[6] A court may also order an adverse evidentiary inference. If the court orders an adverse evidentiary inference as a sanction, the judge may instruct the jury that the evidence that has been destroyed would have been unfavorable to the party responsible for its destruction.[7] This type of instruction casts the party who destroyed the evidence in a negative light and could result in a negative verdict or much higher damages.

IV. New Safe Harbor Rule

One of the most important reasons for you to establish a formalized procedure for destroying documents is that the Amended Federal Rules establish a safe harbor that will protect a party from sanctions. This rule provides that if an organization has a reasonable system for destroying data that is always followed, as long as there is no pending litigation or reasonably anticipated litigation, sanctions will not, absent exceptional circumstances, be issued against the organization for destroying electronic data.[8] For a party to have the best chance of protection under this new provision, an organization must make sure that it has a carefully drafted and comprehensive policy for the retention and destruction of electronically stored data. If a key piece of electronically stored evidence is deleted and an organization does not have a document management policy, or if the document management policy is not followed, that organization will not be protected by the safe harbor rule and will be subject to sanctions.

If you need assistance in drafting a document management policy, or would like your existing policy to be reviewed, please contact Donald Graham at (617) 479 5000 or dgraham@mhtl.com.

---

[5] *Zubulake v. UBS Warburg LLC,* 229 F.R.D. 422, 430 (2004).

[6] *Id.* at 426.

[7] *Id.* at 437.

[8] The amendment to the FED. R. CIV. P. 37(f), Failure to Make Disclosures in Discovery; Sanctions - Electronically stored Information, states in pertinent part, "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

CROWN COLONY PLAZA
300 CROWN COLONY DRIVE
SUITE 410
P.O. BOX 9126
QUINCY, MA 02269-9126

WORLD TRADE CENTER EAST
TWO SEAPORT LANE
BOSTON, MA 02210

(617) 479-5000
information@mhtl.com
www.mhtl.com

ONE MONARCH PLACE
SUITE 1310R
SPRINGFIELD, MA 01144

This alert is for informational purposes only and may be considered advertising. It does not constitute the rendering of legal, tax or professional advice or services. You should seek specific detailed legal advice prior to taking any definitive actions. © 2007 MHTL

Murphy, Hesse, Toomey & Lehane, LLP
300 Crown Colony Drive
Quincy, MA 02169

FIRST CLASS
U.S. POSTAGE
PAID
BOSTON, MA
PERMIT NO. 00461