AAPA

"Legal Issues and Record Retention"

May 15, 2013

SML, Inc.
Steve M. Lewis, President and CEO
813.205.2850
stevemlewis@msn.com
www.smlinfo.net

TABLE OF CONTENTS

CORPORATE OR PUBLIC RECORDS

To address the complexities associated with Corporate or Public Records management, a comprehensive records and information management program is an essential component of any business entity, public or private. It is, therefore, critical to define the scope of the program; and especially to define the term "record."

Generally, *Records* means all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other material, regardless of physical form or characteristics or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business. Generally format, media type or duplication does not affect record status of information created or received. The recommendations contained within this Paper apply to hardcopy as well as digital records, unless otherwise noted. Generally, the Port should select media types for retention based on economy and efficiency, with lengthy retention implications in mind.

Copy of Record vs. Duplicate Records

An immediate problem will be the identification of copy of record (or record copy, or retention copy) vs. duplicate records. **Copy of Record** means the record specifically designated by the Port as the official, retention copy. **Duplicate Record** means all reproductions of copy of record prepared simultaneously or separately, which are designated by the Port as not being the copy of record. The Port should adopt the policy that the office of origin for *internally* generated documents holds the copy of record while receiving offices have duplicates. For *externally* generated records received by the Port, the office, which performs the last administrative act, should be recognized as holding the copy of record. This will prevent accidental destruction of records as misidentified duplicates since the copy of record is maintained per the appropriate schedule.

Email

Email often engenders considerable confusion relative to Corporate or Public Records Law. Retentions are not written for media types. Email is a media type and has no specific retention. The retention for email is content driven. Retentions are written for informational content by record series title.

The fact that information can be made or received electronically does not change the obligation of a Port and employees to direct and channel such official

business information so that it can be properly recorded. Email records created or received in connection with the transaction of Port business are public records.

SCHEDULING

Scheduling is a process whereby Ports establish minimum retention schedules for all Port record series titles. These retention schedules address the **administrative, legal, fiscal and historical values** for records and constitute a minimum retention period.

Mandatory Requirements

Scheduling is the heart of the Records Program, and in order for the Records Program to be legally sufficient, **the scheduling process must be carefully documented and approved**. The **program must be systematic** and **comprehensive**. It is for this reason, in part, that the Record must be so carefully defined and categorized. The Records Program must address all records, regardless of media type or physical characteristics. To selectively apply the program is to invite adverse inference in litigation. The **program must also be developed during the normal course of business** - again, not developed for specific records for specific reasons. **The working papers used to develop the Program, and especially those used to develop the retention schedules must be maintained permanently**. Each retention schedule and disposition document must be **approved and signed** through a regular process.

As retention periods are met, the **records must be destroyed**. Again, the program must include all records and intent must be followed. Records may be maintained longer than approved retention schedules, however, for each such instance documentation should exist to justify not destroying records per existing retention schedules. Units that wish to maintain records beyond the Port's approved Retention Schedules should provide written justification for the destruction delay. This justification must be reviewed by the Port Records Officer for approval or disapproval. If approved, the written justification should be attached to the appropriate Disposition List.

The Agency must maintain the program and continue to designate a Records Officer. **There must be ongoing program control**. **There must be a way to terminate all records destruction**.

DISPOSITION

Disposition is the application of approved retention schedules to record series titles. By far, the most economical solution to public records management is to destroy based on approved retention schedules. Records should be destroyed as soon as legally possible.

Spoliation

Spoliation is the intentional destruction, or significant alteration of evidence. When spoliation is established, an inference may be drawn that the evidence destroyed was unfavorable to the party responsible for its destruction - the spoliator. This obviously includes "records."

Generally, in order to be "evidence," the party responsible for the destruction must know, or should have known, that the items were relevant to pending or imminent litigation. If the items are not, then they are not evidence and their destruction is not spoliation.

Spoliation can constitute obstruction of justice. Spoliation can result in sanctions in court beyond the inference referred to above. If it rises to the level of attempting to perpetrate a fraud on the court, it may result in the dismissal of an action or other summary judgment. Careful adherence to approved retention schedules, and correct application of the Port's Disposition List will virtually eliminate the potential for spoliation.

The disposition form is maintained within the Port and is a permanent record. Lists need also to be maintained in a similar fashion for other disposition options to include conversion to microfilm or digital images. Each Disposition List should be sequentially numbered. Further, each Disposition List must include only one intent.

The Disposition List must represent *actual* destruction, hence the need to destroy all present accumulations eligible. This includes all media. If paper records are destroyed, yet digital records of the same information and record series title are maintained, the Disposition List is incorrect. Ending dates must be amended to accurately depict accumulations not destroyed. As new Schedules are approved for the Port, add these titles and appropriate dates to the List. If source documents relative to destruction are produced (certificates of destruction from recyclers, land fill tickets, etc.) attach these.

Duplicates should only be created for administrative or convenience purposes and then discarded when that purpose is terminated. Every effort

should be exercised to create only those records required, driven by business process.

Media Options

The primary source for determining what is and is not admissible into evidence in trial is the applicable Evidence Code, in Florida for example, **Chapter 90, F.S.** There are some other statutory provisions that can apply as well, particularly with regard to "electronic records." The Federal Rule of Evidence is similar.

Administrative hearings must also be considered. The rules of evidence are generally much broader in those proceedings, the requisite foundation for admission being relevance.

The problem is as discussed: there are too many possible exceptions that can swallow the rules depending upon the innumerable, particularized circumstances that may be attendant to a specific episode. However, the bottom line is, the law has done a good job of recognizing and keeping up with the fast pace of change technology has wrought with regard to the creation, duplication and storage of documents, records and writings. The statutes and rules are generally very technology friendly. There are probably few instances in which a reliable document, electronic or otherwise, is going to be excluded from the record because of some arcane requirement of an "original" piece of paper. Authenticity is the real issue now, and so long as there is some evidence, testimonial or otherwise, that the document is what it is purported to be, in most instances, it will be admitted into evidence. Each jurisdiction must be examined for these particulars.

Metadata

Metadata is receiving particular attention and perhaps points to the greatest vulnerability during discovery. Metadata is data about data - information about a particular data set which describes various attributes such as authorship, creation, modification, and/or format. Federal Rules provide, in part for the discoverability of Metadata. Rule 34 of the Federal Rules of Civil Procedure applies to electronic data compilations from which information can be obtained only with the use of detective devices. Further, Rule 26(a)(1)(B) of the Federal Rule of Civil Procedure provides in part discovery of “data compilations.”

In Florida, the Supreme Court allowed for the discoverability of metadata, for example; a move expected to take place globally. This issue will continue to evolve but points to the need for a comprehensive disposition effort as a regular component of the Port’s record life cycle.

Vital Records Protection

Vital records are those records critical to the delivery of services on a day-to-day basis. Vital records are necessary to continue operations. Vital records do not necessarily have a long retention, as is the common misconception; nor are vital records necessarily confined to any one unit - all units likely maintain some vital record.

The first step in establishing a vital records program is to identify the agency's vital records. Vital records must be identified and protected *before* a disaster. Records to consider include: current contracts; leases and agreements; accounts payable (including payroll) and accounts receivable; current operating budgets; purchase orders; lists of former key personnel (to act as temporary replacements for current employees out of commission as a result of a disaster); current operating procedures; and applications and operating systems. This is unlikely a complete list; inventory and File code implementation data must be used to complete the identification process. The identification process must be ongoing to detect new vital records, or other changes as requirements are adjusted.

After identification, the next step is duplication. The most effective way to safeguard information is by duplication. There is no substitute.

Duplication is followed by dispersal. Dispersal takes two forms: natural and planned. Natural dispersal already occurs. Additionally, back-ups rotated off-site are examples of natural dispersal. Therefore, the need for rigorous off-site storage facility specifications is apparent.

Planned dispersal then fills the gap allowing the protection of the agency's vital records, provided the identification process has been complete. It is important to adopt a simple approach to Vital Records Protection utilizing the following steps:

1. Identify
2. Duplicate
3. Disperse

Off-site storage facilities should be located away from traditional hurricane paths and above flood zones, therefore, away from the coast.

Digital Backup

Every record, even digital equivalents, must be destroyed if represented as such on the Port's Disposition List. **Backups serve to restore data, and should not be seen as a preservation effort**.

Data Processing Recovery

A data processing recovery plan is fundamental given a Port's dependence on data processing to provide vital services; its geographic location and local weather influences; and the continued potential for terrorism, vandalism and accident. Disasters are often geographic in nature. It is possible staff may not be able to access any existing facility. Traditional DPR is remote. Provided digital backups are intact, data processing recovery is possible.

Critical applications must be duplicated and dispersed as described above. In the event of a data processing emergency, the plan may then be implemented.

Investigate the use of a *Hot Site*, a *Cold Site* and a *combination* of the two. Ensure the selected vendor is not overwhelmed with users from a single geographic location. Interlocal agreements for mutual aid are not recommended.