Presentation Paper

For

Session 10: Automated Document Management Systems

Miami, Florida

AAPA
2012 Port Finance Seminar

April, 19th, 2012
10:15 – 11:30 a.m.

SML, Inc.
813.205.2850
stevemlewis@msn.com
www.smlinfo.net

TABLE OF CONTENTS

	Page
Retention Scheduling and a Records Management Plan	3
Dispositioning	3
Digital Imaging	4
Vital Records Protection	4
Data Protection/Security	5
ADDITIONAL INFORMATION	6

Automated Document Management Systems

An Automated Document Management System **must be part of an overall Records Management Plan**. The Plan must be written, it must be systematic and it must be comprehensive. It must also be in accordance with **all applicable legal requirements**. Efficient imaging solutions must consider selection of data sets, activity, retention, security, protection, restoration and sometimes data processing recovery. Clearly, at a conference such as this with international representation, it is impossible to be specific relative to legal requirements. Therefore this presentation has focused on a best practices approach.

Retention Scheduling and a Records Management Plan

Record Retention Scheduling is the heart of the Records Plan, and in order for the Records Plan to be legally sufficient, **the scheduling process must be carefully documented and approved**. The **Plan must be systematic** and **comprehensive**. It is for this reason, in part, that the Record must be carefully defined. The Records Plan must address all records, regardless of media type or physical characteristics. To selectively apply the Plan is to invite adverse inference in litigation. The **Plan 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 Record Retention Schedules must be maintained permanently**. Each retention schedule and disposition document must be **approved and signed** through a regular process.

The Port must maintain the Plan. **There must be ongoing program control**. **There must be a way to terminate all records destruction**. There needs to be control at the highest level and staff must be assigned specific responsibilities. There is usually a **Records Management Officer** assigned to oversee the Plan.

Dispositioning

As retention periods are met, the **records must be destroyed**. Again, the Plan 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.

Digital Imaging

The selection of documents for conversion should be **based on activity** and the need to **distribute across a network or to web enable**. Imaging is not generally a cost effective option merely to reduce physical storage of paper. If possible, create documents in a digital environment and avoid conversion. Conversions must **meet or exceed and legal standards or requirements** to ensure digital reproductions may legally replace paper documents. Unless there are legal requirements to the contrary, open formats such as PDF are preferred. Conversions must be documented when paper output is replaced. Again, ensure legal standards for output and format are met or exceeded and that sufficient documentation for conversion and replacement and process are in place to satisfy any legal standard or requirement. The best "safe harbor" is a rigorous set of policies and procedures which are then adhered to for all data sets throughout the Port.

Digital documents require **content management** otherwise they quickly become swallowed by an ever increasing volume. No conversion project should begin without a **carefully constructed index** and content management solution. Images should be **parsed based on retention** into containers for efficient destruction. If images with vastly different retentions are co-mingled, Dispositioning efforts are frustrated. Indexes should be functionally and organizationally based. Data sets transcend organizational structure.

Digital records must be protected with **limited access** yet available. **Pass words and read only** solutions must be in place. The credibility of the data must be protected.

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 Port'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 and record drawings to possibly include related project file documents.

This is unlikely a complete list. 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. Imaging may prove to be a cost effective duplication effort.

Duplication is followed by dispersal. Dispersal takes two forms: natural and planned. Natural dispersal already occurs. Information is routinely sent to other entities or administrative authorities. Additionally, a microfilm operation that produces security film stored off-site and magnetic tapes 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 Port's vital records, provided the identification process has been complete. It is possible 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.

<u>Data Protection/Security</u>

Digital records must be **duplicated for preservation**. There must be a **Data Processing Recovery Plan**. Individual users should only write to the network and discontinue the use of personal hard drives for data storage. **Backups serve to restore data, and should not be seen as a preservation effort**.

A **data processing recovery plan** (DPR) 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 DPR plan may then be implemented.

Digital images with retentions that may exceed the life expectancy of platforms and drives may be worth candidates for Computer Output Microfilm. Microfilm is not technology dependent and is readable with low grade technology. Microfilm images may also be scanned back into a digital environment. Microfilm can be a very cost effective long term solution as a backup to digital images.

ADDITIONAL INFORMATION

SML, Inc.
www.smlinfo.net

Law.Com
www.law.com

Federal Supreme Court
www.supremecourtus.gov

AIIM
www.edocmagazine.com

ARMA
www.arma.org