The Importance of Creating and Maintaining an Electronic Records Management Process
Contributed by Bob Gregg, Employment Attorney with Boardman & Clark law firm

We live in an electronic society. Virtually all transactions and all records are electronic. Our business and personal conversations are increasingly electronic. There is an electronic trail to almost everything.

All organizations are now required to have a process to categorize, preserve and be able to produce electronic records in litigation. Sometimes, years later.

If you do not yet have a system, this is not something you should think about "getting around to sometime." *It is required!* It has been required for the past several years. The courts are now assessing sanctions of up to $1 million or even granting summary judgment without trial against organizations which just "hadn't gotten around to" developing an effective and comprehensive Records Management Policy and Process. The same sanctions apply to those who did develop a process but then failed to reassess and keep it up to date with changing technology. They should have known their policy and procedures were now antiquated and ineffective. They pay the price.

Both federal and most state court systems have adopted electronic discovery rules. The federal rule is Rule 26(a), which requires that employers disclose, at the beginning of litigation and prior to any discovery by plaintiffs, a copy of or a description by category and location of any documents (paper or electronic) that may support its claims or defenses.

Absence of computer records creates the appearance that one is trying to hide the truth. It can create the presumption that any unproduced record should be viewed as an admission of fault. This created a $2.1 million verdict against the employer in *Arndt v. First Union Bank* (N.C. Ct. App., 2005).

Employers lose cases and are sanctioned by the courts because they did not preserve email and other electronically stored information (ESI) even before an actual lawsuit is filed. A sanction of $175,000 was imposed for deleting emails after the company should have been on notice of a potential claim (legal counsel, HR and IT failed to effectively communicate). *Zubulake v. UBS Warburg LLC* (S.D. NY, 2003). The defendant may have to bear the full cost of retrieval and restoration of improperly deleted electronic records. [$236,000 in *Rowe Entertainment v. William Morris Agency* (S.D. NY, 2002); over $1 million in *Medtronic Sofamor Danek v. Michelson* (W.D. Tenn., 2003).

Other sanctions for spoliation include:

- You pay penalties;
- The court "suppresses" your evidence;
- Presumption of guilt; and
- You lose! Court grants summary judgment due to your bad faith.

ESI includes all "writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained." So this is much broader than just the computer. It includes: •Computer use (intranet and internet); •Telephones; •Cell phones; •Text messages; •Tapes, CDs, disks; •Locaters/global positioning; •Electronic calendars; •Message systems, including voicemail.

Each year, the list changes with technology. Don't forget paper records, as well. All records are included in the discovery rules, but record keeping is now overwhelmingly electronic. Records include: •Reports; •Graphics; •Electronic files; •Charts; •Records; •Contracts; •Drafts and redrafts; •Calendars; •Network access records; •"Documents of any kind."

ELEMENTS OF A POLICY AND PROCEDURE

A records policy and procedure should cover:

- Creation of records (including prohibitions on what not to have on the system);

- Retention and security (including back-up storage media);
- Retrieval (and authenticity); and
- When and how to destroy.

This system should comply with all relevant laws and regulations, not just the court discovery rules. Various laws require keeping records in different ways. Medical information, I-9s, personal identity information, customer financial dates and much more must be kept with security and confidentiality. Other records require no security. Some records are "public" and must be kept open for all to access. The organization may have its own internal concern for trade secrets versus its "public" communication. It is important to know which are which and have coordinated protocols to assure each is generated and stored properly.

There are different statutes of limitations regarding how long different types of records must be retained and requirements can vary from state to state. Labor records must be kept for at least two years. However, Worker's Compensation cases can have a 12-year statute of limitations. A contract can have a six-year statute of limitations. Hazardous chemical records may have to be kept forever. Again, it is crucial to know these requirements, identify and categorize records properly, retain and be able to retrieve them for the proper time before any destruction.

Develop and keep updated the specific protocols for destruction for each category of records. There is a "safe harbor" in the discovery rules. There are no penalties or sanctions if records are disposed of according to a written plan, which is followed consistently, under the control of trained professionals and which allows sufficient time for anticipated claims to be filed before any destruction. Again, this should, at a minimum, track the basic statutes of limitation for various types of records and potential cases.

The records policy and protocol should specify who is responsible for retention and who has specific, and sole, authority to destroy each type of record. There should then be double checks before actual destruction.

Finally, records policies should not only address network storage, but should also account for ESI stored on individual personal computers and other devices.

THE LITIGATION HOLD

Rule 26 also requires you to freeze the electronic system and preserve all ESI when you are "on notice" that there may be litigation. The rule is about preserving information when on notice that there may be litigation. This does not mean waiting until an official summons and complaint is served upon you. It does not mean when a letter from a government agency is received. Instead, the obligation arises when there is any practical reason to believe future litigation might occur over an issue.

So, the "may be" can be triggered by any dispute with a vendor or customer that goes beyond a casual disagreement (*i.e.*, letters start to be exchanged over the issue), any letter from an attorney; anytime an employee is fired during economic times where the next job is hard to find; any accident causing personal injury or property damage. These and more events should prompt one to freeze the system and inform all involved to not delete anything without authorization. Once "on notice," the hold should stop destruction of any relevant records for the duration of the litigation.

DEVELOPING A POLICY AND PROCESS

An effective policy and process requires serious assessment. It is not something which can be copied from some forms manual and plugged in. There must be detailed analysis of your own organization, its operations, business, the extent and type of electronic communications and records.

There are some good starting points. The American Records Management Association has its GARP (Generally Accepted Recordkeeping Principals) model. International Organization for Standardization (ISO) has ISO 15489-1 guidance. However, these are simply the beginnings; a framework which must then be modified and made applicable to your organization.

Who should be involved? The critical actors are external IT consultants, internal IT staff, legal counsel, Human Resources, heads of the departments which generate records, safety and compliance staff. Not all have to be involved in every stage of policy and procedure development. However, the IT consultants, internal IT staff and legal counsel are crucial at all phases of development and implementation.

External IT advisors and providers can be the most helpful. With an overview of many organizations, these professionals have experience and may have good starting models. This saves you from reinventing the wheel.

These providers are also familiar with your operation and in a position to help customize any model to your operation. Once your policies and practices are in place, they will also be in a position to efficiently update your systems as new technology is adopted.

Information storage and retention is becoming more and more complex. This often means using external providers for storage. It certainly means getting professional advice on the equipment, systems, upgrades, etc. needed for the records management system.

The internal IT staff has to oversee and operate the system. They must train people about the system and must enforce compliance. No system works without the involvement and commitment of your IT personnel.

Much of the records management requirements are legal compliance and litigation driven. Legal counsel should have input and overview of all parts. Legal counsel should have a lead role in the Litigation Hold, retrieval and production of information phase, deciding how broad the hold should be and when it may end.

REVIEW AT LEAST ANNUALLY

Technology changes and current decisions expand, or limit, the scope of records management requirements. Outdated management programs result in liability. Stay up to date!