CORPORATE RECORD RETENTION IN AN ELECTRONIC AGE (Outline)

David J. Chavolla, Esq. and Gary L. Kemp, Esq.
Casner & Edwards, LLP
303 Congress Street
Boston, MA 02210

A. Document and Record Retention Preservation Policies Are Part of an Overall Document and Record Management Policy

1. Business operation considerations
   a. control information creation and growth
   b. facilitate access to necessary information
   c. protect integrity and availability of critical business information and data
   d. facilitate orderly disposal of documents that are no longer required in order to save time, space and money

2. Legal principles
   a. statutory and regulatory requirements for organization based on locations, business operations and activities
   b. common law obligations to preserve evidence regarding actual or reasonably anticipated litigation
   c. contractual obligations

3. Professional standards of records management
   a. trade and service organization standards
   b. trade practice standards
      (i) ANSI (American National Standards Association)
      (ii) AIIM (Association for Information and Image Management)
      (iii) ARMA (Association of Records Management Administration)
      (iv) NIST (National Institute for Standards and Technology)
      (v) ISO (International Organization for Standardization)

B. Legal Requirements

1. Statutes and regulations
   a. Internal Revenue Code
   b. State and federal environmental statutes
   c. Labor and employment laws
   d. Criminal statutes that punish obstruction
   e. Industry-specific statutes and regulations that impose unique document retention requirements

(i) Regulatory tagging
(ii) SEC (Securities and Exchange Commission)
(iii) NASD (National Association of Securities Dealers)
(iv) Sarbanes-Oxley Act of 2002

f. Proposed Changes to Rules of Civil Procedure
g. Statutes of limitations
h. Codes of ethics and professional rules

2. Common law duties of preservation
   a. Doctrine of spoliation, i.e., improper destruction of relevant evidence
   b. Adverse inference instruction

C. Coordination of Electronic Management with Privacy and Related Use Policies

1. Protection of trade secrets and competitive commercial information

2. Statutes and regulations addressing privacy rights of individuals
   a. FACTA (Fair and Accurate Credit Transactions Act of 2003) requires destruction of certain consumer information
   b. HIPAA (Health Insurance Portability and Accountability Act of 1996) imposes restrictions against improper disclosure of covered personal information

3. Protection of personal data in the European Union (EU)
   a. Charter of Fundamental Rights of the European Union, Article 8

D. Expanded Retention Obligations Under Sarbanes-Oxley Act

1. Criminalizing the Destruction, Alteration and Falsification of Records in Federal Investigations, Bankruptcy Cases and Official Proceedings
   a. Section 802 provides for fine or imprisonment up to 20 years for anyone who knowingly "alters, destroys, mutilates, conceals, falsifies or makes a false entry" in any record or document with intent to impede, obstruct or influence the investigation or administration of any matter within the jurisdiction of a federal department or agency or any bankruptcy case. *See* Title 18 of U.S.C. § 1519.
   b. Section 1102 establishes the same penalty for anyone who corruptly "alters, destroys, mutilates or conceals" a record or document with intent to impair its integrity or availability for use in an official proceeding.

2. Updating Federal Sentencing Guidelines Related to Obstruction of Justice

a. Section 805 of the Act commanded the U.S. Sentencing Commission to review and amend Sentencing Guidelines.

3. Significant Expansion of Record Retention Requirements for Auditors of Public Companies
   a. Section 101(c) of the Act established a Public Company Accounting Oversight Board to oversee the audit of public companies
   b. Section 103(a)(2)(A)(i) commanded the Board to adopt auditing standards that require accounting firms to "prepare and maintain for a period of not less than 7 years audit work papers and other information related to such reports in sufficient detail to support the conclusions reached in the reports."

E. Recently Adopted Changes to Federal Rules of Civil Procedure Regarding Discovery of Electronically Stored Information.

1. Mandatory early discussion of electronically stored information.

2. Limits on production of documents that are not reasonably accessible due to undue burden or cost.

3. Identifying formats for production of electronically stored information.

4. "Safe Harbor" limit on sanctions.

5. Importance of legal counsel's knowledge of record storage technology.

F. Elements of Effective Document Retention Policy

1. Organizational constituents
   a. Management
   b. Administrative Staff
   c. Legal Counsel
   d. Auditors

2. State objectives and purposes

3. Basic requirements of policy
   a. Retain records long enough to meet retention requirements
   b. Determine location of all offsite electronic documentation maintained by employees (PDAs, home computers, Blackberries, etc.) and centralize wherever practical
   c. Be able to locate records when needed

d. Ensure records can be protected when needed for examination or litigation
e. Destroy records promptly and uniformly when retention requirements are met
f. Tag records according to non-retention requirements
g. Rapid discovery duties under Sarbanes-Oxley
h. Privacy obligations under HIPAA and FACTA
i. Secure destruction obligations

4. Describe organizational responsibility for implementation of policy and designate responsible individuals including "records management officer(s)"
   a. Separate content management and technology custodian functions may be delegated to different individuals
   b. Periodic compliance review may be necessary
   c. Any program must include clear and effective guidance to employees how to identify and maintain required records

5. Identify document and record types the Company generates and retains and which are subject to the policy. Important business records include:
   a. Corporate governance materials (minute books, stock records)
   b. Corporate policies
   c. Tax records
   d. Financial information
   e. Intellectual property
   f. Personnel records
   g. Insurance policies
   h. Contracts and agreements
   i. Official correspondence

6. Identify materials whose preservation is unnecessary and may create needless storage costs and liability exposure
   a. personal emails
   b. Drafts
   c. Newsletters and certain non-essential publicity materials

7. Know where documents and records are located

8. Know who owns and controls each record type

9. Establish retention schedules – know when records become obsolete and can be disposed.

10. Establish systematic procedures for disposal or destruction of documents and records.

11. Establish guidelines for suspending document destruction

12. Audit organization compliance with retention policy.

G. One-Size Retention Policy Does Not Fit All Organizations – An Organization's Information and Records Policy Should Be Realistic, Practical and Tailored To The Unique Circumstances Of The Organization

1. Relevant factors
   a. Nature of the business
   b. Size and organizational structure
   c. Legal and regulatory environment
   d. Organizational culture
   e. Distributed or centralized nature of records and information within the organization
   f. Historic business practices and procedures of the organization

2. Management policy needs to address in a practical and flexible manner the differences in an organization, business needs, operations, IT infrastructure and regulatory and legal requirements

H. Impact of Technology on Creation, Retention and Destruction of Information and Records

1. Identifying, capturing and managing electronic information and records may be a more difficult task than for paper records

2. Electronic records should be kept for the same length of time as paper records

3. Primary responsibility for an electronic record rests with its owner

4. The owner is responsible for assuring that all records are properly authenticated and for preserving "contextual" information such as date and time of creation, origins in the organization and recipients of the records in order to validate authenticity of the document

5. Electronic documents must be stored so as to be retrievable by author and personnel

6. Records officer must be contacted when work station is retired or assigned to a new owner. Records officer must supervise any alteration or removal of documents in this situation.

7. Rules must be in place regarding transition or use of business records and information on employee's home computer.

8. Each storage medium, e.g., tape or disk, must be retained as long as the longest retention period of any record contained therein.

9. Use write-once storage to store documents that need to remain unchanged throughout their life.

10. E-mails and attachments may be covered under various categories under the policy, and must therefore be organized for storage and retention under the policy

11. Emerging technical solutions may obviate a number of previously required steps in classifying data.

12. When software application is retired, associated records must be retained in retrievable, usable format

13. Organization needs to consider impact on retention program of proposals to migrate to new technologies or applications. Arrangements should be made to i) print and save hard copy instead of electronic records, ii) convert electronic record into a more widely used format, or iii) keep and properly store necessary hardware and software so that data can be read and printed.

14. Electronic records sent to off-site storage facility must be accompanied by a content label on the storage medium and a destruction date

15. Programs, program listings and other electronic data processing devices must be retained for the duration of the data they support

16. When ownership of accounts change, passwords and security access to applications and documents must be changed appropriately

17. E-mail disclaimer must be attached

18. Appropriate policies for automatic destruction of personal e-mails should be considered

19. Retention policy should consider whether to preserve metadata for purposes of authentication, security, data integrity, search, retrieval and analysis

I. Destruction of Records

1. Over retention is a major problem. Once records have been retained long enough to meet a regulatory or valid business requirement, they start to become a liability and should be disposed of in a consistent manner.

2. Challenges with e-mail management
   a. Email is over retained, backed-up and archived
   b. People make inappropriate statements in e-mail messages
   c. Organizations do not distinguish between e-mail "records" and "non-essential communications"
   d. Employees are given undue discretion in setting retention and destruction practices
   e. E-mail retention standards seldom exist and are not uniformly applied

3. When is e-mail the official version of a record type instead of a conventional version?

4. What processes, procedures and e-tools can be used to ensure compliance with prescribed retention periods?

5. What processes, procedures and e-tools can be used to ensure relevant e-mails can be identified and accessed when needed?

6. Existing e-mail and file systems were never designed for records management. Back-up and archiving is typically designed only for disaster recovery. Information is subject to multiple duplication (on desktops and .PST, NSF files as office documents; on servers and e-mail systems; and back-up tapes in different locations within an organization). Organization needs to systematically purge information that should be destroyed while selectively retaining information that is required for conducting business or is subject to legal retention requirements.

7. Key considerations in reviewing decisions to destroy records
   a. Eliminate local .PST files which are typically used by Microsoft® Outlook to store email and attachments on a local PC
   b. With local .PST files there is no centralized control over what files get deleted, and remaining files are discoverable
   c. System must be highly customized to ensure retention of documents needed for business or which subject to legal hold requirements, while complying with Company purge policy
   d. Tape record cataloging and restoration are critical to identify data location

e Centralized, single-instance storage is needed to minimize storage requirements and facilitate access to information

f. Discovery from the archive is a mandatory requirement of all systems

8. Review best practices for tape retention and management

J. Practices and Procedures Regarding Suspension of Destruction

1. Suspension of normal destruction of records and information may be necessary under certain circumstances
   a. Actual or anticipated litigation
   b. Government investigation or audit
   c. Preservation orders in litigation
   d. Certain business contexts: mergers and acquisitions; bankruptcies; intellectual property review

2. Organization must be able to anticipate circumstances that will trigger suspension of normal destruction procedures
   a. Government investigation
   b. Service of complaint or petition commencing litigation
   c. Third party request for documents
   d. Knowledge of events likely to result in litigation
   e. Party possessing evidentiary records has notice of relevance

3. Identify persons in organization with authority to suspend normal destruction procedures and impose legal hold

4. Identify specific responses issues which may need to be addressed by the organization
   a. How to identify potentially responsive records
   b. Who collects and coordinates records retention and where and how will records subject to legal hold be stored?
   c. Is there a particular need to preserve legacy records and information on back-up medium or system

5. Legal holds in particular situations should be tailored to the legal requirements of the case, and should apply only to the life of the litigation, investigation, audit or other circumstances giving rise to the suspension

6. Organization should document steps taken to implement a legal hold

K. Selection of Document Retention Software