909 - Spotting & Resolving Legal Issues in Your Company's Records Management Policy

Wendy Curtis
Senior Associate
Fulbright & Jaworski LLP

Martin Grant
SVP & Chief Compliance Officer
Federal Reserve Bank of NY

Dawn Haghighi
Attorney
Princess Cruises

Mark Harrington
General Counsel
Guidance Software, Inc.

Marty Provin
Executive Vice President
Jordan Lawrence Group

Faculty Biographies

Wendy Curtis

Wendy Curtis is a senior associate at Fulbright & Jaworski L.L.P. in the Washington, DC office. Ms. Curtis has expertise in the identification, preservation, collection, review, and production of massive amounts of electronically stored information. Her practice has expanded to include records management and electronic discovery as a member of the firm's electronic discovery and information management practice group. Ms. Curtis' records management and e-discovery experience includes: serving as national e-discovery counsel; advising clients in litigation readiness; management of discovery at a national level, including electronic discovery and complex document production; creation of record retention schedules; creation and implementation of preservation notice policies; creation and implementation of record management policies and programs; and records management and preservation notice employee training. Ms. Curtis also has extensive experience in complex litigation, class actions, pharmaceutical products liability, and health law litigation.

Ms. Curtis is a member District of Columbia Bar Association, Healthcare Businesswomen's Association, ARMA International, and the Sedona Conference and does pro bono adoptions for the Children's Law Center.

Ms. Curtis received a B.A., cum laude, from the University of New Hampshire and is a graduate of the University of Maryland School of Law.

Martin Grant

Martin C. Grant is the chief compliance and ethics officer of the Federal Reserve Bank of New York. As a senior vice president in the legal group, he has responsibility for the compliance function, the ethics office, and the records management function.

Mr. Grant is co-chair of the criminal and enforcement litigation sub-committee of the ABA's business law section.

Mr. Grant is a graduate of Princeton University and Harvard Law School.

Dawn Haghighi
Attorney
Princess Cruises

Mark Harrington

Mark E. Harrington is general counsel and assistant corporate secretary for Guidance Software, Inc., a Pasadena, CA public company that provides software and services for digital investigations related to eDiscovery, incident response, and document management.

Prior to joining Guidance Software, Mr. Harrington was a senior attorney at Intel Corporation, where he worked on complex intellectual property agreements, mergers and acquisitions, and general corporate matters. Previously, Mr. Harrington was in-house counsel, with Trillium Digital Systems, Inc., a developer and licensor of telecommunication source code protocol software. He began his legal career working on complex litigation and electronic discovery matters for the law firm of Munger, Tolles and Olson in Los Angeles.

He is a member of the board of directors for ACC's Southern California Chapter.

Mr. Harrington received his B.A. from the University of California, Los Angeles and his J.D. from Southwestern University School of Law.

Marty Provin

Marty Provin is executive vice president of Jordan Lawrence, a specialty consulting firm focused on assessing, developing, and enforcing corporate records policies and practices. He works with Jordan Lawrence clients in developing effective strategies to leverage technology and process in order to achieve legally defensible corporate records programs.
Prior to joining Jordan Lawrence, Mr. Provin was in the technology industry where he worked with Fortune 500 companies in developing solutions to manage workflow and increase efficiency.
He regularly speaks to the legal and information technology communities on managing records to mitigate risks while improving efficiency.

Legal Requirements and Sources

Mark E. Harrington
General Counsel, Guidance Software, Inc., Pasadena, CA

Legal Retention Requirements

- Statutory Requirements
- Regulations
- Company Specific
- Statute of Limitations for matters that your company routinely faces
- Case Law

ACC's 2007 Annual Meeting: Enjoying the Ride on the Track to Success October 29-31, Hyatt Regency Chicago

Statutory Requirements

- Title VII
- HIPAA
- GLBA
- Sarbanes Oxley
- U.S. Patriot Act
- Privacy Laws (CA SB 1386, FACTA)

Title VII

- ADA and FMLA
  - Documents of "employment actions"
    - Hiring
    - tests
    - Promotions
    - Transfers
    - Warnings
    - Layoffs
    - Terminations

One year from taking action or final disposition of the charge or lawsuit if such is filed

HIPAA Records

- **HIPAA**
- All HIPAA Privacy Notices, authorizations, plans, company policies, complaints, resolutions, training materials, sanctions, governmental investigations, disciplinary actions against employees, related to PHI.
- All requests by and responses to individuals with respect to (I) amending or correcting PHI (ii) accounting for PHI disclosures (iii) inspecting and copying PHI (iv) restricting the use and disclosure of PHI and (v) receiving confidential communications of PHI
- **Retention Period**
- **All of the documents listed above shall be retained for a minimum of six years from the later of: (i) the date the document was created, or (ii) the date the document was last in effect.**
- **Retention Format**
- The documents will be maintained in either electronic or hard copy format. If the documents are in electronic format that format will comply with all applicable statutes including HIPAA and ERISA.

Sarbanes Oxley

- **Sarbanes Oxley**
- Sarbanes Oxley criminalizes, for the first time, the destruction of records regardless of whether there is a pending governmental inquiry at the time the records are destroyed--and even if the documents are destroyed in accordance with an otherwise appropriate document retention program.
- The actual language of the act states "Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both."
- SECTION 802 (applies to Auditor): Seven (7) Years

Gramm Leach Bliley Act

- Requires financial services institutions to create privacy policies, which must be shared with customers and how such information can be shared between financial institutions
- Generally, the Act does not contain express language regarding document retention time periods.
- However, safe to say that documents related to the establishment and maintenance of a privacy policy, program, communications with customers and other financial institutions about such plan, should be kept indefinitely.
- When assessing retention of financial records, companies should also abide by state regulations.

U.S. Patriot Act

- Requires all "financial institutions" to establish anti-money laundering programs. Applies to banks, bankers, brokers, insurance companies, and individuals involved in real estate closings.
- Like GLBA, safe to say that records related to such money laundering programs should be retained indefinitely.

Privacy Laws

- Proper Handling and Disposal of documents containing sensitive or personal information about customers and employees (Social Security, credit, license, bank or other personal information)
  - California 1386
  - Fair and Accurate Credit Transactions Act

Regulations

- OSHA
- Federal Wage and Hour Laws
- SEC

ACC's 2007 Annual Meeting: Enjoying the Ride on the Track to Success October 29-31, Hyatt Regency Chicago

OSHA

- OSHA requires employers to keep records of both medical and other employees who are exposed to toxic substances and harmful agents. Employers must maintain these records for **30 years**.
  - Other examples:
    - Company logs of "occupational illnesses" **5 years**
    - I-9 forms under Immigration Reform and Control Act **3 years after hire or 1 year after term**

Wage and Hour Laws

1) Employee Information, Payrolls, Individual and Union Agreements, Plans, Trusts and Notices.
   Three (3) Years

2) Supplementary Employment records time cards, wage rate tables, work time schedules, order shipping and billing records, job evaluations, merit or seniority systems, or matters which explain basis for wage differentials to employees of opposite sex, deductions or additions to pay.
   Two (2) Years

Fair Labor Standards Act (29 CFR 516.2-516.6 and 516.11-29).

SEC

- Company Auditors now required under Rule 2-06 of Regulation S-X to implement Section 802 of the Sarbanes-Oxley Act of 2002, to hold audit-related records for seven (7) years.
- SEC Rules 17a-3 and 17a-4 require broker-dealers to create and preserve a comprehensive record of all securities transactions the broker-dealer effects and of the securities business in general. The SEC views these requirements as the primary means of monitoring compliance with the securities laws, including anti-fraud provisions and financial responsibility standards.

Company Specific

- Consent Decrees
- Litigation Holds and Settlements
- Contractual Commitments and Audit Rights given to 3rd parties
- Industry Regulations (Maritime, Banking, Industrial requirements)

Claim Statute of Limitations

- White Collar Crime
- Fraud
- Misrepresentation
- Breach of Contract

Statute of Limitations

- **White Collar Crime and Fraud**
  - CA: 4 years (Cal Penal Code Sec. 801.5)
  - NY: 2 years from discovery or 6 yrs after fraud (McKinney's CPLR Sec. 213)
- **Securities Violations (SOX Sec. 804)**
  - 2 years after discovery or 5yrs after violation
- **Misrepresentation**
  - CA: Generally, no SOL (CA Civ Pro Sec. 340.6)
  - NY: Generally, 3 years (Sec. 214)
- **Breach of Contract**
  - CA: Four Years (CA VIV PRO Sec. 340.6)
  - NY: 6 years (McKinney's CPLR Sec. 213)

Recent Case Law

Wendy Butler Curtis
Senior Associate, Fulbright & Jaworski, Washington, DC

Developing Technologies

- Preservation of Voicemail
  - *Del Campo v. Kennedy*
  - *In Re Seroquel Prods. Liab. Litig.*
- Digital Databases
  - *Burkybile v. Mitsubishi Motors Corp., et al.*
- Instant Messaging (IM)
  - *FDIC Guidance on Instant Messaging*

Preservation Notice Cases

- *Valdez v. Town of Brookhaven*
  - Preservation orders are burdensome and expensive and in the absence of a clear need should not be entered.
- *Google, Inc. v. Am. Blind & Wallpaper Factory, Inc.,*
  - "A willful indifference" to fulfilling discovery obligations warrants evidentiary and monetary sanctions.
- *Capitano v. Ford Motor Co. Maremont Exhaust Prods., Inc.,* and *Gibson v. Ford Motor Co.*
  - Preservation notices are privileged.

Preservation Obligations

- *In re NTL, Inc. Sec. Litig.*
  - "Utter failure" to preserve relevant documents and ESI was "at least grossly negligent," and adverse inference instruction granted.
- *Miller v. Holzmann*
  - Government failed to comply with its duty to preserve, however, dismissal was not an appropriate sanction.
- *Doe v. Norwalk Comty. Coll.*
  - In order to take advantage of Rule 37(f)'s good faith exception, a party needs to have a routine system in place and act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business.

Expert Witnesses

- *In re Zyprexa Prods. Liab. Litig.*
  - Court ordered Plaintiff's expert witness to "immediately preserve any and all documents and information including, but not limited to, all computer(s), hard-drives, other electronic storage media, hardcopy documents, emails, e-documents, text messaging, instant messaging, phone records and voice mails, that refer or relate to Zyprexa."
- *Bedford, LLC v. Safeco Ins. Co.*
  - Hard copies of electronic drafts from testifying experts are discoverable. However, there is "no legal principle that would require a testifying expert witness to separately retain all electronic drafts, including those that were overridden or subsumed during the drafting process."

Production of Backup Tapes Denied

- *Bank of Amer. Corp. v. DR Int'l Bus. Ins. Co.*
- *Cache La Poudre Feeds, LLC v. Land O' Lakes, Inc.*
- *Georgia Dep't of Agric. v. Griffin Indus.*
- *In re Celexa and Lexapro Prods. Liab. Litig.*
- *Oxford House, Inc. v. City of Topeka*
- *Palgut v. City of Colorado Springs*

Courts Ordering Production of All Requested Backup Tapes

- *Wachtel v. Health Net, Inc.*
- *Best Buy Stores, L.P. V. Developers Diversified Realty Corp.*
- *Peskoff v. Faber*
- *In re Veeco Instruments, Inc. Sec. Litig.*
- *Metro Wastewater Reclamation Dist. v. Alfa Laval, Inc.*
- *Disability Rights Council of Greater Washington v. Wash. Metro. Area Transit Auth.*

Limited Production of Backup Tapes and Cost-Sharing

- Courts Ordering Preliminary Inquiries or Limited Production of Backup Tapes
  - *Semsroth v. City of Wichita*
  - *AAB Joint Venture v. United States*
  - *Wells v. Xpedx*
- Courts Ordering Cost-Sharing of Production of Backup Tapes
  - *Analog Devices, Inc. v. Michalski*
  - *Quinby v. WestLB AG*
  - *O'Bar v. Lowe's Home Ctrs., Inc.*

Metadata

- *Kentucky Speedway v. NASCAR*
  - Court declines to order production of metadata
- *Williams v. Sprint*
  - *Sprint I* (2005)
    - Court ordered production of metadata on grounds that metadata is contained in documents as maintained "in the ordinary course of business"
  - *Sprint II* (2006, post-Amendment)
    - Court declined to order production of metadata

Creating Records Management/Retention Program To Comply With Legal Req.

Dawn Haghighi
Director, Corporate Counsel Compliance Governance for Princess Cruises and Cunard Line

ACC's 2007 Annual Meeting: Enjoying the Ride on the Track to Success October 29-31, Hyatt Regency Chicago

Sample Training Materials

- Document Collection Checklist
- Document Collection Process Checklist
- Sample Hold Notice
- Sample RR Policy
- Record Management Training and Definitions

Practical Solutions and Technology To Enable In-house Counsel To Implement and Enforce RM Program

Martin Grant
SVP & Chief Compliance Officer, Federal Reserve Bank of NY

The Goal at FRBNY

- Establish a Bank-wide program for the management, retention, protection, and timely destruction of records and information.
- Manage ALL records, regardless of format

Technology Factors Driving E-Discovery Complexity

- Challenges of Preservation, Collection and Production
- No one solution for all issues
  - Unstructured v. structured data
  - Metadata
  - 100s if not 1000s of databases and applications
  - Proprietary technology
  - Multiple Locations (12 Reserve Banks)

The Foundation: Policies

- Records Management Policies
  - Umbrella
  - Local
- E-Record Policies and Procedures
  - Metadata
  - EDiscovery

Policies (Cont'd)

- Communication-Specific Guidelines
  - Email
  - Blogs
  - Meetings, Telephone Calls & Recordings
- Other Relevant Policies
  - Employee Privacy
  - Information Security Manual

ACC's 2007 ANNUAL MEETING

Autonomy Search Engine (E-Discovery)

- Indexes and Searches multiple repositories
- Reduces Cost and Time required to conduct Discovery efforts in unstructured repositories
- Governed by procedures that include Legal, IT, and business areas

ERMS (Electronic Records Management Submission) Tool

- Developed internally to address email, e-records, and imaged records
- Leverages existing systems
  - Hummingbird DM
  - Hummingbird Webtop
  - Lotus Notes
- Classifies records according to records retention codes

ACC's 2007 Annual Meeting: Enjoying the Ride on the Track to Success October 29-31, Hyatt Regency Chicago

ERMS Tool

- Submission Process
  - user-defined vs. auto-classification
  - Permits delegated authority; assistants can handle these tasks for executives
  - Automates process of requesting retrieval and re-filing of boxed paper records

Imaging

- For appropriate records:
  - Provides distributed access
  - Enhances search and retrieval capabilities
  - Accommodates business contingency needs

Challenges and Limitations

- Maintenance of numerous components
- May be a "temporary solution" as the DM/RM and Electronic Content Management (ECM) markets are in continuous flux
- Legacy records that pre-date the system
- Accommodating "new technologies": blogs, IMs, and web content

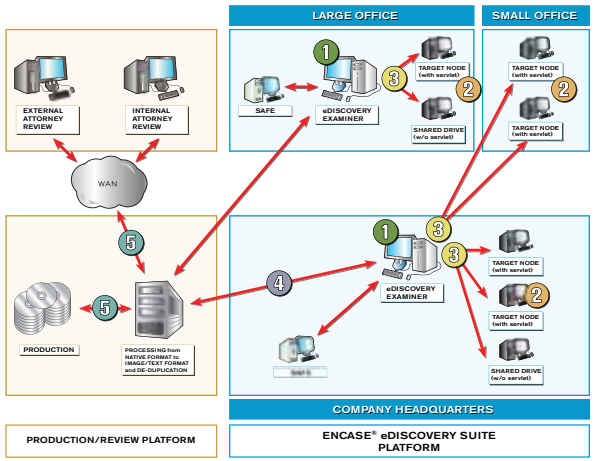
Staff Training

- Vital to the SUCCESS of any program
- Elements to be included:
  - RM Policies and Retention Schedules
  - Use of the ERMS
  - Records disposal and hold procedures
  - Privacy
  - Careful Communication

Resources

- ABA Legal Technology Resource Center, Electronic Discovery - http://www.abanet.org/tech/ltrc/fyidocs/ediscovery.html
- ARMA - http://www.arma.org
- Electronic Discovery Reference Model (EDRM) - http://www.edrm.net
- Federal Judicial Center, Education Programs and Materials (this includes, available to download, Managing Discovery of Electronic Information: A Pocket Guide for Judges, Barbara J. Rothstein; Ronald J. Hedges; Elizabeth C. Wiggins, 2007.) - http://www.fjc.gov
- Ken Withers - http://www.kenwithers.com
- The National Archives - http://www.archives.gov/records-mgmt
- The Sedona Conference - http://www.thesedonaconference.org

GUIDANCE SOFTWARE | SOLUTIONS



1. Examiner machine sends search requests for potentially relevant data to any number of computers
2. Powerful search for only potentially relevant data performed on target computers
3. Resulting files, including metadata – a collection feature unique to EnCase software – are collected and sent to Examiner machine
4. Data collected and preserved by Examiner (including metadata) in Logial Evidence Files are then sent in native format to the review/production platform
5. Review/production platform makes data available for attorney review, redaction, bates-number and production

It is important for organizations to be proactive and gain control of the information on their networks; however, they often do not have the ability to accurately enforce their records retention policies. Organizations that implement a standardized process to proactively enforce records retention policies reduce risk and increase efficiency during auditing, records management, and eDiscovery tasks. EnCase eDiscovery Suite enables organizations to proactively audit their networks to identify and eliminate out-of-compliance documents.

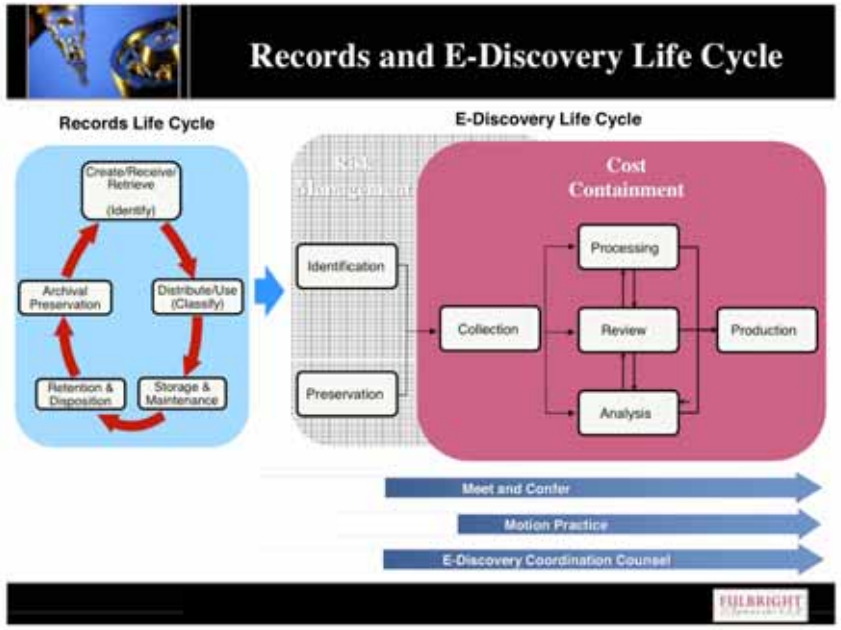
EnCase eDiscovery Suite completely automates the records management, eDiscovery and auditing process. eDiscovery Suite radically reduces the costs associated with these processes while enabling proactive and accurate enforcement of records retention policies. The process based approach of eDiscovery Suite enables agencies to implement a standardized process by which to overcome all auditing challenges.

For more information, please contact Guidance Software at (626) 229-9191, or visit us on the web at www.guidancesoftware.com

Guidance SOFTWARE

About Guidance Software (GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough and effective computer investigations of any kind, such as intellectual property theft, incident response, compliance auditing and responding to eDiscovery requests—all while maintaining the forensic integrity of the data. There are more than 20,000 licensed users of the technology, and thousands of investigators and corporate security personnel attend Guidance Software's forensic methodology training annually. Validated by numerous courts worldwide, EnCase software is also frequently honored with top security awards



FULBRIGHT & Jaworski L.L.P.

E-Discovery First Steps: Identifying and Preserving Potentially Relevant Electronic Information

The first hours, days, and weeks after receiving notice of a litigation matter may pose great challenges and present high risks, particularly regarding identification and preservation of potentially relevant electronically stored information (ESI). With tight time constraints and minimal information, companies and their counsel must take steps to understand the issues, identify and preserve sources of ESI, and protect the company from inadvertent destruction of relevant information.

The list of considerations below is intended to serve as a quick reference guide for companies and their counsel during the initial crucial hours and days. The precise steps that are taken will vary depending on the nature of the litigation, the issues presented, and the company's resources, practices and technology infrastructure. Many companies are taking steps to put response plans in place *before* litigation hits. An effective response plan, one that considers the issues identified below and is implemented quickly upon notice of a litigation matter, can have a substantial impact on the outcome of the matter.

Understand Scope Of Litigation and Communicate With Company Representatives.

- Review complaint, subpoena(s) or other available documentation.
- Communicate nature of the litigation and obligations to corporate representatives from legal, information technology (IT), risk management, business units, human resources or other departments.

Consider Use Of Outside Expert.

- Consider whether an outside consultant is advisable for identification, preservation and/or collection of potentially relevant information.
- If so, identify and retain the outside expert as quickly as possible, and include the outside expert in developing and implementing the data identification, preservation and collection plan.

Identify Sources Of Potentially Relevant ESI.

- Identify key employees most likely to have potentially relevant data.
- Interview information technology (IT) representatives and other employees to determine what information is stored on networked email and non-email accounts, personal computers, laptops, voice mail, databases, etc. Gain an understanding of the company's IT environment and infrastructure.
- Determine whether relevant information may be within the individual employee's control, such as personal digital assistants, flash drives, personal email accounts, personal cell phones, etc.

Take Initial Steps To Preserve Active ESI.

- *Preservation Notice to Employees and Third Parties.*
  - Prepare and issue a written directive to employees who may possess relevant material, instructing individuals regarding their preservation obligations. Keep in mind that the Preservation Notice may be discoverable.
  - Identify as broadly as possible the documents and ESI to be retained and the employees who may possess such documents.
  - Consider third parties who may possess documents under the company's control and whether they should receive a letter or notice requesting preservation.
  - Consider having recipients of the Preservation Notice acknowledge their receipt and understanding of the memo.
  - Develop a plan to reissue the Preservation Notice periodically and to re-evaluate the scope for any needed alterations and expansion as more information about the litigation becomes available.
- *Routine Disposal Practices.*
  - For designated individuals, consider suspending routine data disposal practices, such as auto delete processes for email accounts.
  - If feasible, implement suspension of auto delete processes for designated individuals as quickly as possible.
- *Network Accounts for Email and Network Directories for Non-email.*
  - Consider whether litigation risks and company resources justify creating a forensically sound copy or mirror image of network email accounts and network directories of employees likely to have responsive documents. Segregate and preserve any copies made in a secure repository.
  - If employees' network accounts and directories are not imaged, develop an alternative preservation plan for networked data sources. Balance data privacy concerns against the need to preserve relevant information quickly.
- *Desktops/Laptops.*
  - Consider creating a forensically sound copy or mirror image of the hard drives of key players' desktops or laptops. Determine appropriate timetable for copying data, and segregate and preserve any copies made in a secure repository.
  - If key players' hard drives are not imaged, consider alternative means of preserving relevant information and develop an alternative preservation plan. Again, balance data privacy concerns against the need to preserve relevant information quickly.
- *Databases/Structured Data.*
  - Determine whether relevant data may exist in databases, such as a document management system, and whether that data may be subject to modification or deletion.
  - Develop a plan to preserve unaltered data, which may include "locking" documents to prevent inadvertent alternation or deletion.
- *Collection of Preserved Data.*

- Develop a reasonable and defensible plan for collection of data that has been preserved. It may not be necessary to collect all data that has been preserved.
- Collection methodology may vary depending on type of litigation matter, size and complexity of case, perceived risks and costs, company resources, and technology infrastructure.

Develop Plan For Backup Tapes and Legacy Data.

- Investigate the company's archival and backup routines and existence of potentially relevant legacy data.
- Many companies routinely recycle disaster recovery backup tapes, causing data on the tapes to be overwritten.
- Consider whether to continue normal recycling of backup tapes, or identify specific backup tape(s) to be withdrawn from the normal rotation cycle and preserved during the pendency of the litigation or until agreement can be reached.

Consider Departed And Departing Employees' Data.

- Develop a procedure for preserving data of departing employees who may have responsive documents on their computers.
- If the company has a practice of wiping clean the computer hard drives of departing employees so the computers can be redeployed, image hard drives before redeployment or preserve the original hard drive during pendency of the litigation.

Negotiate Issues With Opposing Counsel As Soon As Possible.

- Develop and discuss a reasonable plan for preservation and collection with opposing counsel as early as possible.
- The Meet and Confer process can be an effective tool to limit scope of discovery and drive desired results.
- If agreement cannot be reached, consider motion practice to request a protective order from the court. Volume drives the cost of discovery of ESI, and a strategic focus on reducing volume as early as possible, while meeting discovery obligations, can reduce costs of electronic discovery.

Document Steps Taken To Preserve and Collect Potentially Relevant Material.

- Actions taken now and the reasons for those actions may be questioned later.
- Contemporaneous documentation of rationale for decisions may help demonstrate that reasonable efforts were made in good faith.

Guidance SOFTWARE

Guidance SOFTWARE

Document Retention and Remediation using EnCase® Software
General Guidelines

Enforcement Timeline

Action	Purpose	Date of Deletion
Email Purging	To retain emails, regardless of subject or attachments, only for such time as they continue to have a legitimate business purpose or, as otherwise required by law.	Every Day Emails that are older than three (3) years for Officers, Vice Presidents or Board Members and, Emails older than one (1) year for all other employees, will be deleted from Guidance systems, mail servers and local hard drives.
Collection of Non Email Documents Subject to Destruction	To comply with GSI Document Retention Guidelines	First Friday of Every Quarter
Review Period by Non Email Document Owner	Allow Document Owner a chance to review or re-classify documents subject to destruction	Second Week of Every Quarter
Non Email Document Destruction	Delete document(s) from local hard drives and network server locations	End of Day, Every Second Friday of Every Quarter

1

Guidance SOFTWARE

Retention Timeline
(non Email Documents)

Document Type	**Department Owner**	**Retention Period (after useful life)**	**Digital Storage File Type/Location**	**File Naming Convention** **(Filename)_(Dept). (File Type)**	**EnCase* Retention Enforcement and Remediation**
401k Documents	HR	Perpetual	**Server XYZ**	_HR	**Naming Convention**
Accident reports/claims (settled cases)	HR	7 years		_HR	Date Range Keyword: Accident, Claim
Accounts Payable ledgers and schedules	Finance	7 years		_FIN	Date Range
Accounts receivable ledgers and schedules	Finance	8 years		_FIN	Date Range
Annual Statements	Finance	Permanently		_FIN	Naming Convention
Attachments and Garnishments	HR	2 years		_HR	Naming Convention
Attendance Lists	Training	4 years		_TRN	**Naming Convention**
Audit reports	Finance	Permanently		_FIN	**Naming Convention**
Back-Up Tapes	IT	1 year		_IT	**Naming Convention**

Guidance SOFTWARE

Bank Statements	Finance	7 years		_FIN	Key Words: Bank Name(s)
Business Travel Docs	HR	7		_FIN	**Naming Convention**
Capital stocks and bond records: ledgers, transfer registers, stubs showing issues, record of interest coupons, options, etc.	Corporate	Permanently		_CORP	**Naming Convention**
Case Studies	Marketing	7 years		_MKT	**Naming Convention**
Cash books	Finance	Permanently		_FIN	**Naming Convention**
Charts of accounts	Finance	Permanently		_FIN	**Naming Convention**
Checks (canceled checks for important payments, special contracts, purchase of assets, payment of taxes, etc. Checks should be filed with the papers pertaining to the underlying transaction)	Finance	Permanently		_FIN	**Naming Convention**
Checks (canceled except those noted	Finance	7 years		_FIN	Key Words: Bank

above)					Name(s)
Contracts and leases (expired)		7 years		_LEG	**Naming Convention**
Contracts and leases still in effect	Legal	Permanently		_LEG	**Naming Convention**
Corporate Policies	Corporate	Permanently		_LEG	**Naming Convention**
Correspondence, general		2 years		Dept specific	**Naming Convention**
Correspondence, legal and important matters	Legal	Permanently		_LEG	**Naming Convention**
Correspondence, routine with customers/vendors	All	2 years		Dept specific	**Naming Convention**
CPE Credits	Training	5 years		_TRN	**Naming Convention**
Credit Memos	Finance	7 years		_FIN	**Naming Convention**
Customer Satisfaction Surveys	Technical Support	2 years		_RD	**Naming Convention**
Deeds, mortgages and bills of sale		Permanently		_FIN	**Naming Convention**
Depreciation schedules	Finance	Permanently		_FIN	**Naming Convention**
Drafts (After Final Version Complete)	All	One Month		_DRAFT in title name	**Naming Convention**
Email – Active In Box	IT	Three Years for Officers, Vice Presidents and			Date Range

		Directors; One Year for All Other Employees			
Email Archive – Local Hard Drive and Servers	IT	Three Years for Officers, Vice Presidents and Directors; One Year for All Other Employees *			Date Range
Email Archive Attachments	IT	Three Years for Officers, Vice Presidents and Directors; One Year for All Other Employees			Date Range
Employee personnel records (after termination)	HR	4 years		_HR	**Naming Convention**
Employment applications	HR	3 years		_HR	**Naming Convention**
Export Compliance Documents	Operations	Permanently		_OPS	**Naming Convention**
Faxes (Incoming and Digital Copies)	Facilities	One Week		_FAC	Date Rate, Document Type *.tif, Specific Server
Financial statements	Finance	Permanently		_TRN	**Naming**

(year-end, other months optional)					**Convention**
Fixed Asset Additions and Retirements, Salvage Value	Finance	Permanently		_FIN	**Naming Convention**
General ledgers, year-end trial balances	Finance	Permanently		_TRN	**Naming Convention**
GSA Administration	Operations	7 Years		_OPS	**Naming Convention**
GSA Letters	Training	7 years		_HR	**Naming Convention**
HIPAA Information	HR	Permanently		_HR	**Naming Convention**
Income Tax Returns and Formal submissions responses, payments	Finance	Permanently		_FIN	**Naming Convention**
Instant Messages	IT	None			**Naming Convention**
Insurance Policies	Legal	Permanently		_LEG	**Naming Convention**
Insurance records, current accident reports, claims, policies, etc	Legal	Permanently		_LEG	**Naming Convention**
Intellectual Property Filings and Registrations	Legal	Permanently		_LEG	**Naming Convention**
Internal audit reports	Finance	4 years		_FIN	**Naming**

(miscellaneous)					**Convention**
Inventory records	Operations	7 years		_OPS	**Naming Convention**
Invoices to customers or from vendors	Operations	7 years		_OPS	**Naming Convention**
IRA and Keogh plan contributions, rolloers, transfers and distributions	HR	Permanently		_HR	**Naming Convention**
IT Request Forms	IT	1 year		_IT	**Naming Convention**
Leases	Legal	6 years		_OPS	**Naming Convention**
License Assignments	Customer Service	Permanently		_OPS	**Naming Convention**
License Agreements	Operations	Permanently		_LEG	**Naming Convention**
Media Advisories	Public Relations	7 years		_MKT	**Naming Convention**
Minute books of directors, stockholders, bylaws and charter	Corporation	Permanently		_CORP	**Naming Convention**
Non Disclosure Agreements	All	3 Years		_LEG	**Naming Convention**
Payroll records	Finance	Permanently		_FIN	**Naming Convention**
Perpetual Software Licenses	Legal	Permanently		_LEG	**Naming Convention**

Petty cash vouchers	Finance	4 years		_FIN	**Naming Convention**
Power Point Presentations	All	Three Years		Department Specific	Date Range Document Type *.ppt
Press Releases	Marketing	7 Years		_MKT	**Naming Convention**
Product Manuals	Technical Support	Permanently		_RD	**Naming Convention**
Professional Services Agreements, CERTS, Invoices, Statements of Work	PSD	Permanently		_PSD	**Naming Convention**
Property records, including costs, depreciation reserves, year-end trial balances, depreciation schedules, blueprints, and plans	Finance	Permanently		_FIN	**Naming Convention**
Purchase Orders	Finance	6 years		_FIN	**Naming Convention**
Purchase Orders – Customer	Customer Services	3 years		_OPS	**Naming Convention**
Receiving Sheets	Operations	1 year		_OPS	**Naming Convention**
Register Tapes	_FIN	6 years		_OPS	**Naming Convention**
Retirement and	HR	Permanently		_HR	**Naming**

Pension Records					**Convention**
Returned Merchandise Authorizations	Customer Services	1 year		_OPS	**Naming Convention**
Safety Records	HR	6 years		_HR	**Naming Convention**
Sales Records	Finance	7 years		_FIN	**Naming Convention**
Stock and Bond certifications (canceled)	Corporate	Permanently		_CORP	**Naming Convention**
Subsidiary ledgers	Finance	7 years		_FIN	**Naming Convention**
Tax Exemptions – Customer	Customer Services	7 years		_OPS	**Naming Convention**
Tax returns, revenue agents' reports, and documents relating to determination of income tax liability	Finance	Permanently		_FIN	**Naming Convention**
Time cards and daily reports	HR	7 years		_HR	**Naming Convention**
Trademark registrations, patents and copyrights	Legal	Permanently		_LEG	**Naming Convention**
Tradeshow, Sponsorship and Speaker Bureau Contracts	Marketing	3 years		_MKT	**Naming Convention**

Guidance Software

Travel and Entertainment Records	Finance	Permanently		_FIN	**Naming Convention**
Vacation/Leave of Absence Forms	HR	Permanently		_HR	**Naming Convention**
Vendor documents	All	Life of Contract plus 3 years		Department Specific	**Naming Convention**
Video Clips	Marketing	1 year		_MKT	**Naming Convention**
Voucher for payments to vendors, employees, etc (includes allowances and reimbursement of employees, officers, etc, for travel and entertainment expenses)	Finance	7 years		_FIN	**Naming Convention**
Voucher register and schedules	Finance	7 years		_FIN	**Naming Convention**

* EnCase Software installed on a company network to automate the Document Retention and Remediation Process.

Fulbright Client Alert

NOVEMBER 2006

FULBRIGHT & Jaworski L.L.P.

AND WHILE YOU'RE TAKING OUT THE E-GARBAGE... IMPLEMENTING PROCEDURES FOR NON-CURRENT BACKUP TAPES

The proposed amendments to the Federal Rules, which go into effect December 1, 2006, will dramatically change the way companies create and store backup tapes.[1] To prepare for this change, many companies have already begun to dispose of useless "e-garbage," or non-current, backup tapes.[2] Disposing of these tapes is crucial given the dramatic implications that new Rule 26(b)(2) has for discovery. After December 1, companies will be required to disclose the existence and extent of their backup tapes to the court and to opposing parties where they contain "potentially responsive" electronically stored information. They may also be required to search or sample otherwise inaccessible backup tapes pursuant to court order if an opposing party can show good cause. Owing to the excessive costs associated with restoration and attorney review of backup tapes, which can contain millions of typewritten pages each, companies should do everything possible, keeping in mind any pre-existing preservation obligations, to limit the number of backup tapes they have both before and after December 1.

Even as companies are disposing of backup tapes, some by the thousands, they should be thinking about what to do with the tapes left behind in the metaphorical closet. Disposing of non-current backup tapes should be only the first step in a two-step approach to backup tapes in a post-amended rules world. While companies have started inventorying, analyzing, and disposing of their non-current backup tapes in advance of the anticipated amendments, it is crucial that companies also have plans to track, label, store and eventually dispose of the backup tapes they plan to keep or create after December 1. For many companies, this means creating and executing new records management policies on a company-wide basis, or enforcing compliance with existing records management policies.

Disaster Recovery Backup Versus Archival Tapes

While the focus of this update is disaster recovery backup tapes, understanding the difference between disaster recovery and archival tapes is essential.

According to The Sedona Guidelines:[3]

> Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media. Backup data serves as a source for recovery in the event of a system problem or disaster. Backup data is distinct from "Archival Data."
>
> Archival Data is information that is not directly accessible to the user of a computer system but that an organization maintains for long-term storage and record-keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives or network servers.

As the definition suggests, disaster recovery tapes, also called backup tapes, go stale as soon as a new set is made. Once stale, these tapes can and should be disposed of or recycled, absent a litigation hold. Archival

1 This article pertains to disaster recovery (a.k.a. backup) tapes. Archival or offline storage tapes must be treated according to a company's record retention schedule and policies.

2 See Take Out the E-Garbage...by December 1, Fulbright & Jaworski L.L.P. E-Discovery & Information Management Update, March 2006, located at: http://intranet.fulbright.com/images/publications/EDiscovery%20and%20Information%20Mgt%20Update%20-%20EGarbage%20-%20March%2020061.pdf

3 THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE, Sept. 2005, App. F.

tapes, on the other hand, are designed for long-term retention and should only be disposed of when legal, regulatory, and business retention obligations have expired. Thus, as companies create and deploy procedures for backup tapes, it is important to emphasize that archival tapes should be treated differently and in accordance with record retention schedules and policies.

The Backup Rotation Cycle

Unfortunately, many companies lack a concrete policy on just how long disaster recovery backup tapes can and should be maintained. Clearly, the time when companies could keep backup tapes without a firm retention period in place has come and gone. While the old trend was to retain backup tapes for years, or indefinitely, or even just for an arbitrarily determined period, owing many times to misguided fears concerning the inadvertent destruction of documents, the new trend should be to:

- Adopt and rigorously implement a company-wide policy clearly stating the company backup tape rotation period and the procedures used to cycle active tapes through rotation and destruction
- Shorten the backup tape cycle if a company currently keeps tapes longer than 35 days (5 weeks), unless there is some specific business purpose or litigation hold that requires a longer period
- Require that special backups (e.g., snapshots prior to server upgrades) be distinguished from disaster recovery backup tapes, and be destroyed as soon as maintenance is complete and the installation is stable
- Strictly limit the retention of tapes to the period specified in the backup tape policy, unless a litigation hold is in place that applies to a certain tape
- Give appropriate notice to IT personnel that any newly adopted four or five week rotation cycle is intended to replace, not supplement, *all* old backup practices
- Prohibit freelance backup practices such that IT personnel must present a concrete purpose for creating non-standard backup tapes and senior IT personnel must sign-off on such tapes before they are created
- Require approval from senior IT personnel and in-house legal before a backup tape may be used to fulfill a restore request from an employee or client

A company that currently lacks records management policies stating the specific length of its backup tape rotation cycle should create and execute a company-wide policy on this issue as soon as possible. Having a specific and uniform backup tape rotation cycle is important, but it is meaningless without proper implementation.[4] Until a specific rotation cycle is put into operation, a company is only creating more and more non-current backup tapes that will need to be audited.

Companies that have existing backup tape rotation cycle policies may want to consider shortening those cycles to 35 days (5 weeks) or even 28 days (4 weeks). Both of these lengths are becoming increasingly common, as they allow companies to maintain only as few backup tapes as necessary. Keeping a large number of backup tapes is generally unnecessary, as disaster recovery backup tapes become stale as soon as the next set is made. For all of the reasons discussed previously in relation to the new Rule 26(b)(2), a limited tape inventory will help companies to reduce tape budgets, storage costs, potential business disruptions and expenses during discovery.

4 While an established backup tape rotation cycle only applies to disaster recovery tapes, companies should not overlook the fact that archival and off-line storage tapes should also be thoroughly addressed in separate records management policies.

Once in effect, use auditing and other compliance techniques to ensure backup tapes are kept only as long as the backup tape policy permits, unless a litigation hold applies to a tape. Generally speaking, litigation holds always supersede standard records management practices, including customary disaster recovery tape cycles.

Special backup tapes are a unique category of backup tape that are created for a limited and temporary purpose, such as snapshot tapes made when reconfiguring applications, during server migration, or during server upgrades. Special backup tapes should be immediately destroyed once they are no longer required for the project for which they were created unless, of course, they are subject to a litigation hold.

A company must also verify that IT personnel adopt any newly implemented rotation cycle for disaster recovery backup tapes as a consistent and uniform practice. They should not merely supplement older practices with the new, creating multiple and different rotation cycles. Instead, they should cease outdated practices and carry out only the newly adopted rotation cycle and any other accompanying policies. The company should also prohibit freelance backup tape creation, ensuring that the only backup tapes made are those specifically authorized by the company's records management policies. Finally, a company should also have appropriate procedures and forms in place for IT personnel to use before utilizing a backup tape to fulfill a restore request for lost data made by an employee or client. Formal, written approval from senior IT personnel and in-house counsel is essential, as restore requests can convert a data source from inaccessible to accessible under the amended Federal Rules. Ideally, these approvals should be rarely given, because the more a company uses its backup tapes as archives rather than disaster recovery tapes, the weaker its defense will be against the cost of restoring backup tapes to meet ordinary discovery requests in litigation.

Labeling & Tracking Tapes

The importance of labeling and tracking all of a company's tapes, whether disaster recovery or archival, cannot be understated. An effective and organized labeling and tracking system should encompass several elements:

- Use of a tracking or inventory software with the capability to track all of a company's tapes
- Use of barcodes or other computerized scanning system
- Detailed labeling and a comprehensive inventory

Some companies currently utilize tracking and inventory backup software that allows them to easily know where their backup tapes are and what they contain. Companies that do not currently use such software should commence using it as expeditiously as possible. However, mere software is not enough. Each tape should be labeled with a barcode upon its creation. This barcode will ideally work in conjunction with the company's tracking and inventory software to allow a user to quickly know the tape's name, date, and content. In addition, each tape should have information on the tape label (or the company may choose to use the inventory) regarding the specific contents of each tape and the record retention categories that apply to the tape. For example, the description of data should be detailed to a level such that if a company received a document request for "all of Sally Smith's e-mails from October 2006," the company would know exactly where to find them. A concrete expiration date should also be included on the label and in the inventory.

Procedures should exist to require that tapes be added to the inventory and labeled immediately upon creation. These procedures will help ensure that all of a company's archival and live backup tapes are identified and accounted for at all times, facilitating disclosure under the new Rule 26(b)(2). Companies should also have clear procedures covering backup and archival tapes inherited during mergers or acquisitions. These tapes should be analyzed and, subject to the company's policy, added to the company's inventory immediately upon

the merger or acquisition. Related procedures should guarantee that all of an acquired company's tapes are accounted for, including those that may be stored off-site.

Finally, keeping a detailed inventory and knowing what types of tapes it has at all times will help prevent a situation in which a company owns unique format tapes that it cannot read or restore. For example, many companies have kept older VAX or Wang tapes that no one in the company is able to read. Not only do many companies lack inventories that contain information on these tapes, but they did not keep the technology required to read them. Beyond just being inaccessible under the amended Federal Rules, many of these tapes may be entirely unreadable or readable only by outside vendors at great expense to a company. Thus, if a company must retain legacy data for business or litigation hold purposes, procedures should be in place to either maintain hardware and software that is converted or migrate data to a readable format, such as PDF.

Disposition of Non-current Backup Tapes as They Expire

If a company has accumulated a group of non-active disaster recovery backup tapes no longer part of a backup rotation cycle, it is important under the new Federal Rules that the company determine if any of the tapes have expired (that is, are no longer needed for business, regulatory, or litigation purposes). If so, they should be properly destroyed. In order to accomplish this, a company should have in place policies and procedures that:

- Allow IT personnel to know when tapes expire
- Document the disposition procedures
- Grant definitive disposal authority to a small number of senior individuals

IT personnel should routinely identify and dispose of expired tapes that are not part of a backup rotation cycle. A well-created inventory database, combined with sound labeling, will make identification of such expired tapes easier. A company should also have in place procedures for identifying, segregating, and storing tapes subject to litigation holds and for disposing of such tapes once holds are lifted. Once identified (for example, on a daily or weekly basis), IT personnel should be responsible for disposing of the expired tapes. However, there should be in place a documented process for disposal.

A company should have a company-wide Disposal/Destruction Authorization Form that is consistent with the company's records management practices. This form should be signed by both in-house legal and records management before actual disposal takes place, and a copy of the form should be kept on file. A small number of individuals within the company should have ultimate disposal authority. These people should be responsible for signing off on all disposal decisions, using the proper authorization form, before disposal, and should be ultimately responsible for ensuring that all disposals are made in accordance will company policy, including the policies that all companies should have governing destruction, retention requirements, and litigation holds. Although it may sound tedious, having a paper trail to account for the disposal of expired tapes is key to success in future litigation.

Rule 30(b)(6) Witnesses and Meet and Confer Conferences

Developing records management policies and procedures that encompass the above issues will also help companies in the long term to prepare Rule 30(b)(6) witnesses and plan for meet and confer conferences required under Rule 16. The following preparations will also help companies to be ready for litigation:

- Memorialize how long it takes to retrieve tapes from storage, particularly off-site storage

- Memorialize any available internal information regarding the estimated time and cost to restore tapes
- Create a complete map of your IT infrastructure, and identify exactly what is (and what is not) backed up on a regular basis, checking for any gaps in backup procedures as you go
- Detail who is responsible for the backup of each system in each of the company's offices
- Memorialize all of the procedures described above and monitor compliance

Conclusion

Even while companies dispose of non-current backup tapes in anticipation of December 1, they also need to consider how to handle the tapes left behind or created after December 1. Disaster recovery tapes kept after they become stale increase technology expenses, storage costs, and litigation exposure. When used for their intended purpose, disaster recovery tapes can and should be disposed of pursuant to a company's specific backup tape rotation cycle policy. Those disaster recovery tapes that a company maintains should be labeled and tracked to ensure eventual disposal and proper disclosure during discovery. Procedures should be in place to ensure that inaccessible disaster recovery tapes are not converted into accessible data sources through use to retrieve lost data. Procedures should also be in place to ensure that tapes are disposed of as they expire, and that any and all disposals are tracked. Finally, companies should memorialize the knowledge it gains during the tape audit and planning process for use in preparing 30(b)(6) witnesses and planning for Rule 16 meet and confers.

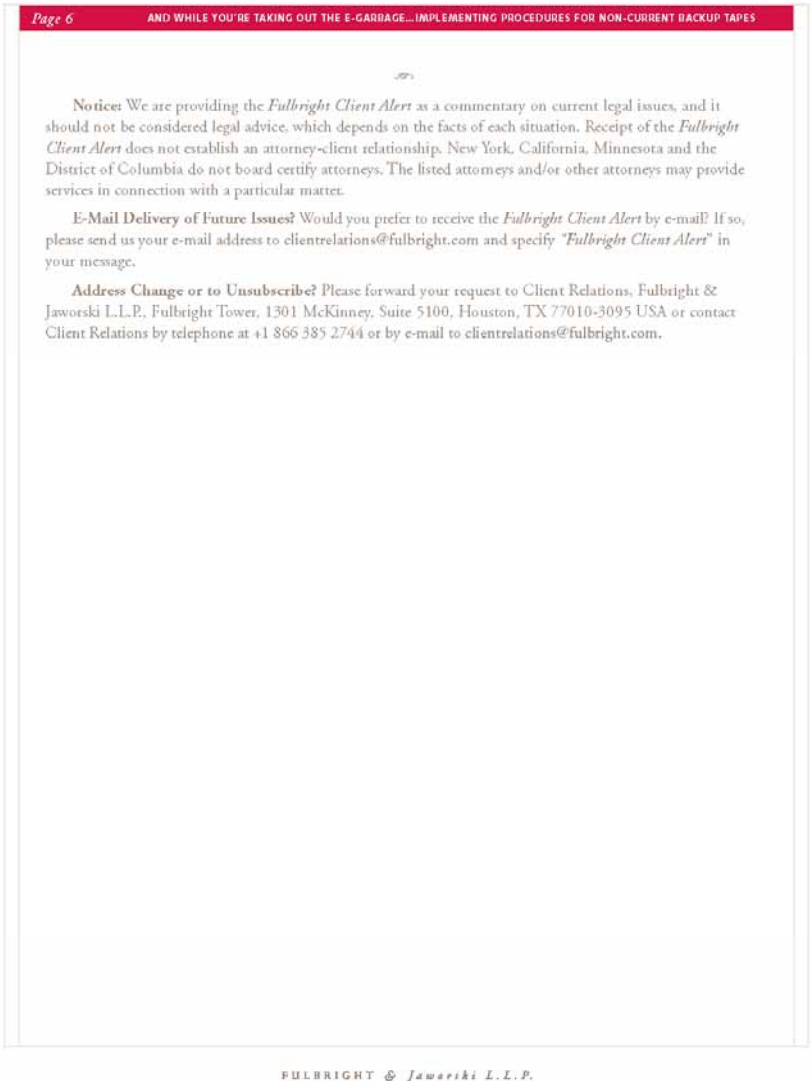
If you need additional information concerning this Alert, please contact Bob Owen, Wendy Butler Curtis, Emily Frangos, Keith Angle, or Sarah Warlick.

Contacts

Bob Owen	*Partner*	*212 318 3070*	*rowen@fulbright.com*
Wendy Butler Curtis	*Sr. Associate*	*202 662 4651*	*wcurtis@fulbright.com*
Emily Frangos	*Sr. Associate*	*212 318 3364*	*efrangos@fulbright.com*
Keith Angle	*Counsel*	*713 651 3534*	*kangle@fulbright.com*
Sarah Warlick	*Associate*	*202 662 4587*	*swarlick@fulbright.com*

Fulbright & Jaworski's E-Discovery and Information Management Practice

Fulbright & Jaworski's E-discovery and Information Management Practice Group is involved throughout the United States in virtually every type of e-discovery and records retention matter. Our experienced and knowledgeable attorneys have counseled companies on their litigation hold policies and processes, formulated records retention schedules, advised on backup tape retention issues, and helped prepare for e-discovery emergencies wherever they might occur. We strive to give practical, reasonable advice that fits the business environments of our clients while protecting them from the adverse consequences that flow from a misstep in this area.



********SAMPLE TRAINING MATERIALS********

RECORDS RETENTION TRAINING

IMPORTANT DEFNITIONS

Active Record

A record that is regularly referenced or is required for current business use.

Business Need

The timeframe during which a business team uses a record for their specific operations.

Convenience Record

Routine information with temporary usefulness, used for communication but not for the documentation of a specific company transaction.

Inactive Record

A record that is not used on a regular basis for current business operations but is still needed by the company.

Legal Compliance

The process or procedure to ensure that the company is following applicable laws.

Life Cycle

The life span or time period from the creation or receipt of a record through its useful life to its final disposition. The five stages in the life cycle of a record include the creation stage, the distribution and use stage, the storage or maintenance stage, the retention and disposition stage, and the archival preservation stage.

Official Version of Record

A record designated as or indicated to be the formal, final or primary draft, whether in print or electronic form, of that record.

Profiler

An individual designated to identify how records are used by a business team, including retrieval prompts; compare old naming practices for records stored with an updated list of standard names; determine naming standards and business needs for each record type; and use the Enforcement Solutions System to classify and retrieve records.

Prepared by Dawn Haghighi, dhaghighi@aol.com

********SAMPLE TRAINING MATERIALS********

RECORDS RETENTION PROGRAM TRAINING
IMPORTANT DEFINITIONS (continued)

Record

Records are defined in various statutes, including the Federal Records Act and the Freedom of Information Act. In general, a record is any written, photographic, machine-readable, or other information created or received that documents activities in the conduct of company business.

Record Hold Notice

A notice requiring all record types identified to be held and secured from destruction and alteration.

Records Retention

The act of maintaining or securing records for future use, and destroying records, pursuant to the policies and procedures of a formally established records retention program.

Retention Period

The period of time during which a record must be retained in a certain location or form. The retention period is governed by operational, legal, fiscal, historical or other business requirements. A retention period may be stated in terms of months or years, and is sometimes expressed as contingent upon the occurrence of an event.

Reviewer

An individual designated to review and approve the work completed by a business team's profiler(s); and use the Enforcement Solutions System to review record type profiles and the retention schedule for the team's records.

Vital Records

Records containing information required for the ongoing operations of the company and needed to re-establish or continue an organization in the event of a disaster; records containing unique and irreplaceable information necessary to recreate an organization's legal and financial positioned preserve the rights of the organization and its employees, customers, shareholders and other constituent groups. Vital records are often maintained permanently.

********SAMPLE TRAINING MATERIALS********

RECORDS RETENTION PROGRAM TRAINING

Why have a records management program?

Sanctions and legal liability that could have been avoided with a proper records management program:

- **Records Storage:** American Express Financial Advisors fined $300,000 for failing to keep customer account statements in the required format (non-rewritable, non-erasable).
- **Records Destruction:** Court imposes $1 million fine on Prudential for records destruction, despite a lack of evidence of willful misconduct, after the company fails to adopt an effective records management policy.
- **Email**: Microsoft faces an antitrust lawsuit based in part on an internal e-mail describing efforts to use viruses in Microsoft products to disable competitors' products.
- **Email**: American Home Products Corporation settles for nearly $3.75 billion, as a result of an e-mail exchange depicting an irreverent attitude toward the potentially harmful effects of its weight-loss drugs.
- **Records Production:** The SEC fines Bank of America $10 million for misleading regulators and stalling on producing evidence in an investigation of improper trading by employees at its securities brokerage.
- **Email / Document Destruction:** Frank Quattrone, former head of a CSFB investment banking division, is convicted of obstructing justice and faces up to 25 years imprisonment for sending an e-mail encouraging the destruction of files while a criminal probe was under way.

CONFIDENTIAL & PRIVILEGED

DOCUMENT COLLECTION PROCESS CHECKLIST *

Prepared By

Dawn Haghighi

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

CONFIDENTIAL & PRIVILEGED

I. Preliminary Considerations

A. Determine the scope of the document collection.
B. Identify privacy issues.
C. Identify applicable laws that apply.
D. Identify, review and secure applicable Company Documentation Retention Policy.
E. Secure a confidential location to secure documents.
F. Assemble a Document Collection Team.
G. Conduct Document Collection Process.
H. Issue Hold Notices.

II. Privacy Issues

A. Identify any applicable privacy issues and potential privacy rights.
B. If needed, secure any consent to review documents or secure acknowledgments executed by employees regarding "No Expectation of Privacy."

III. Assemble a Document Collection Team

A. Attorney-Client Privilege: To preserve attorney-client privilege related to the Document Collection Process, the document collection should be directed by legal counsel.
    1. Document Collection notes may be discoverable and/or utilized in a court proceeding.
    2. To maintain the attorney-client privilege, the Document Collection Process summary should contain the following language: "CONFIDENTIAL: Provided to (in-house attorney or outside counsel) for the purpose of obtaining legal advice, prepared at the direction of legal counsel and in anticipation of litigation."
    3. Other possible privileges:
        a. Work Product Doctrine.
        b. Self Evaluative Privilege.
B. Outside Counsel vs. In-house Counsel: Evaluate the need to retain and use outside counsel as opposed to using in-house counsel to coordinate the Document Collection Process.
C. Transparency: Take steps to ensure the document collection team-members are independent and the collection process appears transparent.
D. Subject Matter Expertise: Identify document collection team-members with subject matter expertise.
    1. For example, determine whether an IT expert or other subject matter expert is necessary to assist with the document collection.

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

CONFIDENTIAL & PRIVILEGED

2. Legal counsel, preferably outside counsel, should retain and direct the work of outside consultants.

IV. Document Collection Process and Preservation

A. Document Collection Process
   1. Identify and secure potential records.
      a) Paper
      b) Electronic
   2. Identify and notify the Record Custodian(s).
   3. Issue Hold Notices to all Custodians and confirm that Custodian understands that it is his/her responsibility to inform all individuals with access not to alter, edit or add to documents.
   4. Identify place to secure records during the Hold Notice Period.
   5. Prepare and create a memorandum describing the Document Collection Process.
      a) Description of record
      b) Time frame
      c) Format
   6. Prepare a written record of the document collection process.

V. Collection Process Interview

A. General Considerations
   1. Identify pertinent individuals or parties related to Document Collection Process.
      a) Employees
      b) Contractors
      c) Third Party Vendors
      d) Storage Companies
   2. Identify pertinent documents related to the individuals or parties described above.
      a) Contracts
      b) Purchase Orders
      c) Invoices
      d) Others
   3. Depending on the magnitude of the document collection process and significance of event at issue, provide the following disclosures at outset of all Document Collection Interviews.
      a) Advise employees that the Company has a responsibility to collect and preserve all documents.
      b) Advise employees that they must provide accurate and truthful information.

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

CONFIDENTIAL & PRIVILEGED

   c) Where appropriate, explain that actions that are viewed as compromising the collection process may result in disciplinary legal action by the Company and/or by law.
   d) Where appropriate, review the Company's Anti-Retaliation Policy. In appropriate circumstances, prepare an Acknowledgment Form for all investigation participants to execute regarding review of Company policies.
   e) Be prepared for responses to tough questions:
      a. May I have legal counsel present?
      b. May I take notes?
      c. May I tape record the interview?
      d. Am I obligated to answer the questions?
      e. Will I be fired?
      f. May I have a union representative present?

B. Conducting Collection Process Interviews
   1. Maintain the Confidentiality of the Document Collection Process. See section III above.
   2. Issues to consider for the interview
      a) In general, questions such as **who, what, why, when, where** and **how** will assist in eliciting the most valuable information. The following can be used as a reference when conducting the interview:
         a. Background information on all participants interviewed in Collection Process.
            i. Name of the person interviewed.
            ii. Dates of employment.
            iii. Identify the employee's title and name of department.
            iv. Identify the name of the employee's manager.
            v. Where appropriate, identify all positions held by the employee and department names or office location.
            vi. Obtain contact information, i.e., telephone number, email address, office telephone number
         b. Information regarding documents
            i. Do you save files to the Company's network?
            ii. Do you create backups of your electronic records or files?
               1. Floppy disks
               2. CDs/ DVDs
               3. Any other locations

*This document only provides general guidance and is not intended to be legal advice. Each investigation should be conducted based on the circumstances of that investigation.

Dhaghighi@aol.com
Dawn L. Haghighi

iii. Can you think of any other location where documents may be found in response to the Hold Notice?
iv. Do you know of anyone else who may have documents that may be in response to the Hold Notice?

c. Distinguish between first hand knowledge and speculation of facts.

3. Documenting the Document Collection Process
   a) Document the start and end time of each search.
   b) Identify where the search was conducted.
   c) Identify what was searched and found.
   d) Identify where it was found.
      a. Electronic documents.
         i. Email
         ii. Inbox
         iii. Calendar
         iv. Sent Items
         v. Personal Folders
         vi. Journal
         vii. Archive Folders
         viii. Public Folders
         ix. Blackberry
         x. Other PDAs (Palm Pilot, etc.)
         xi. MS Office
         xii. Word Files
         xiii. Excel Spreadsheets
         xiv. PowerPoint Presentations
         xv. Hard Drive
         xvi. Other Applications
      b. Paper documents.
         i. Desk File Drawers
         ii. File Cabinets
         iii. Department Files
         iv. Site Files
         v. Other Shared Files
         vi. Stored Files (e.g., LA Records)
   e) Complete Data Collection Checklist.

C. Concluding the Document Collection Process
   1. Provide contact information for person to notify if there are new records identified after the interview.

Dhaghighi@aol.com
Dawn L. Haghighi

2. Notify participant of the Hold Notice and provide copy to participant.
3. Where appropriate, have participant acknowledge receipt of Hold Notice.
4. Notify participant to advise of any new documents retained.
5. Where applicable, inform participant of confidential nature of the collection process.

VI. Finalizing the Collection Process

A. Hold Notice
   1. Distribution of Hold Notice
      a) Issue Hold Notice.
      b) Document who received the Hold Notice.
      c) Confirm that Hold Notice recipient acknowledged receipt and has taken action.
   2. Monitoring Hold Notice
      a) If appropriate, re-issue Hold Notice on a periodic basis.
      b) Obtain confirmation of acknowledgement and receipt of Hold Notice.
      c) Periodic review and communication.
   3. Confirm compliance with Hold Notice.

Dhaghighi@aol.com
Dawn L. Haghighi

SAMPLE

Records Hold [Notice or Alert or Directive]

The Office of the General Counsel has **[learned or has been notified]** of a **[pending or contemplated] [litigation or government investigation or subpoena]** regarding the **[Company]** in the matter of **[ ].** As part of the **[Company's]** Corporate Records Program, you must immediately retain and preserve from alteration or destruction **[including suspending ordinary disposal or alteration]** all records or documents in all media forms (paper and electronic **[including Records stored on removable portable mediums such as, CD, DVD, or flash drive]**) (collectively, "Records") that may be relevant to the **[litigation or that may pertain to the investigation or be responsive to the subpoena**.

[Employees are prohibited from destroying or altering or Under no circumstances may an employee destroy or alter] [relevant Records or any Record that is a relevant] to **[pending or contemplated] [litigation or government investigation or subpoena]**. The Records can only be destroyed after **[the proceeding or investigation]** is **[terminated or concluded]** and the Office of the General Counsel has provided written instructions allowing destruction.

To ensure compliance with this Records Hold **[Notice or Alert or Directive] [you are expected to or you must]** immediately comply with the following directives:

1. Take steps to identify and preserve from alteration or destruction all Records that are known or believed to be relevant. Special attention must be given to identifying and preserving Records that without intervention would automatically be destroyed or erased (such as, emails or voicemail messages).

2. **[Distribute this Records Hold (Notice, Alert or Directive) or communicate the contents of this Records (Notice or Alert or Directive) to all members within your department]** and where appropriate third parties or vendors, whose assistance is necessary to ensure full **[compliance or cooperation]** and fulfillment of the Records Hold **[Notice or Alert or Directive].**

3. Respond within **[forty eight hours]** to certify compliance with this Records Hold **[Notice or Hold or Alert]**.

NOTE: Once the Jordan Lawrence System is up and running then they can go on the Enforcement Solutions and certify on-line.

Prepared by Dawn Haghighi, dhaghighi@aol.com. This is a sample document and is not intended to provide legal advice.

Destruction of relevant Records, even if inadvertent, could seriously prejudice the Company, including having criminal or civil penalties imposed on the Company and/or individual employees who failed to take steps to retain and preserve the Records. If you **[are uncertain or have any questions]** regarding whether a particular Record pertains to a **[pending or contemplated investigation or litigation or may be responsive to a subpoena],** you **[should or must or are required to]** preserve the Record in question and ask the Office of the General Counsel **[or the Corporate Governance Counsel]** for advice.

Failure to comply with this Records Hold **[Notice or Alert or Directive]** could result in disciplinary action including termination of employment **[and where warranted legal action.] * Note Carnival includes a legal action phrase in its Records Policy.**

For more detailed instructions on the preservation of records, please consult the Company's Corporate Records Program.

_____ _____

Signature Date

_____

Title

By signing the above, I certify and represent that I have complied with this Records Hold **[Notice or Alert or Directive.]**

Prepared by Dawn Haghighi, dhaghighi@aol.com. This is a sample document and is not intended to provide legal advice.