

Records Retention: Part I*

by Alan Gutterman**

ISSUE NO. 130
October 2008

* This material was reprinted from *Business Transactions Solutions* (available as a Westlaw database, BTS) with permission from the author.

** Alan Gutterman is a partner at the San Francisco and Silicon Valley offices of The General Counsel (<http://www.thegeneralcounsel.net/>), a provider of interim in-house general counsel and attorney recruitment services. Mr. Gutterman has over two decades of experience as a partner and senior counsel with internationally recognized law firms counseling small and large business enterprises in the areas of general corporate and securities matters, venture capital, mergers and acquisitions, international law and transactions, strategic business alliances, technology transfers and intellectual property, and has also held senior management positions with several technology-based businesses. Mr. Gutterman is also the author of several publications, including *Business Transactions Solutions*, *California Transactions Forms*, *Corporate Counsel's Guide to Strategic Alliances*, and *Corporate Counsel's Guide to Technology Management and Transactions*.

This article covers the general procedures for establishing and administering a records retention program. It identifies the legal and business reasons for establishing a records retention program and describes the steps to be taken to launch and maintain such a program, including the essential elements of the program, policies and procedures, identification and storage of records, establishment of records retention schedules, records destruction procedures, and staffing and administration of the program. An overview of relevant laws and regulations is also included as part of this article, including a discussion of specific records retention requirements. It also includes

continued on page 2

Letter from the Editor.....1

Records Retention: Part I.....1

- I. Practice Considerations.....2
- II. Business Considerations.....7

Dear Subscribers:

In this issue of *Corporate Counsel's Records Retention Report*, we are pleased to provide the first part of a two part article written by Alan Gutterman. This article generally discusses procedures for establishing and administering a records retention program. Part I covers practice considerations, including essential elements of a records retention program, policies and procedures, retention schedules, retention manuals, electronic documents, and a helpful checklist. Part I also discusses business considerations, such as identifying and inventorying business records, staffing, retention periods, and the storage, retrieval, and destruction of documents. Our thanks to Mr. Gutterman for allowing us to share his article with our subscribers.

Very truly yours,
Jeanne D. Wertz
Senior Attorney Editor

checklists for drafting and reviewing comprehensive records retention policies.

In Part I of this article, appearing below, the practice and business considerations of a records retention program are discussed. In Part II, which will appear in next month's issue of this newsletter, legal and tax considerations of a records retention program will be discussed and checklists for drafting and reviewing records retention policies will be included.

I. Practice Considerations

A. Purposes and Advantages of Records Retention Programs

Records retention is an important, if not essential, element of any legal compliance program. In fact, it is impossible for a business to establish and maintain a compliance system without a comprehensive records retention program that is respected throughout the organization and demanded by the senior managers of the company. While the importance of such a program should be self-evident, managers and employees may need to be reminded of some or all of the following specific reasons and advantages:

- All businesses, regardless of size or activity, are subject to at least some substantive laws and regulations that include recordkeeping requirements.
- Records can be, and generally are, used to demonstrate compliance with applicable laws and regulations to law enforcement agencies, government regulators and other parties seeking confirmation of compliance (e.g., prospective investors or other business partners or parties seeking to bring legal action against the company).
- Failure to establish a formal program may lead to inappropriate destruction or retention of records that may cause significant legal and business issues for the company.
- Proper management of records can achieve cost savings for the company with respect to storage requirements and time saved when the need arises to review information included in documents created in the distant past. Time can also be saved by disposing of records that no longer need to be retained, since

such documents would no longer be relevant for discovery purposes in a litigation context.

- Valuable business information about customers and other business partners can be quickly and easily shared within the company if employees know where to find the information.
- A solid records retention program can be an important tool for companies confronted with potential litigation since the company can quickly collect all relevant records and make a determination as to whether there are any "bad facts" that might impact defense or settlement strategies.

In summary, advocates of a formal records retention program rightly argue that the records, and information included therein, are no less valuable than other operational assets of the business and should be afforded the same level of attention and resources as the company devotes to preserving its physical, financial and technological assets.

B. Essential Elements of Records Retention Program

The elements of a records retention program should be organized in a way that facilitates accomplishment of several important goals and objectives for the company:

- Effective facilitation of the management and use of important information generated and received by the company during the course of its business activities. Simply put, the program should make it easy and quick for employees to find what they need to know in order to carry out their day-to-day duties and responsibilities.
- Identification and preservation of all records necessary for the company to satisfy regulatory requirements, fulfill tax obligations, prosecute and defend legal actions, satisfy its contractual commitments, and assert insurance claims.
- Careful definition of the records to be retained and the retention periods for retained records in order to reduce the risk and costs associated with records retention. For example, by eliminating unnecessary records, either because they are not material or they are too old to be relevant, the company can reduce its storage expenses, improve the organization of its

Copyright 2008 Thomson Reuters/West. All rights reserved. *CORPORATE COUNSEL'S RECORDS RETENTION REPORT* (ISSN 1098-0261) is published monthly by Thomson Reuters/West, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Subscription Price: \$210.00 annually. *This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice. If legal advice or other expert assistance is required, the service of a competent professional should be sought.* The information contained herein is based upon sources believed to be accurate and reliable—including secondary sources. Where cases, statutes, or other official materials have been reprinted, we have attempted to provide materials as close to the originals as possible, but we do not purport to publish any documents verbatim. While we have exercised reasonable care to ensure the accuracy of the information presented, no representation or warranty is made as to such accuracy. Readers should check primary sources where appropriate and use the traditional legal research techniques to make sure that the information has not been affected or changed by recent developments.

information, avoid the use of outdated information that can lead to poor decisions, and decrease liability exposure.

The scope and complexity of the records retention program will depend on a variety of factors including the size and type of business and the specific regulatory environment to which the company is subject. The essential elements of a comprehensive program are written policies and procedures that define the business records of the company, facilitate identification and collection of business records, require protection and preservation of records, and establish procedures for destruction of records in a timely and secure manner once the applicable retention period has expired. These policies and procedures should be supplemented by additional information in employee handbooks and regular training of employees on the actions that need to be taken in order for the program to be effective, including manuals and other written materials that can be consulted on a day-to-day basis as questions arise. Another part of the program should be board resolutions and/or formal orders from the senior executives which establish managerial responsibility for the program and allocate suitable human and financial resources to support the program. Finally, there should be plans and procedures for regular monitoring and auditing of the program and each of the specific policies and procedures referred to above.

It is strongly recommended that procedures and guidelines be developed in consultation with recognized experts in the specific areas, as well as knowledgeable and experienced persons from each of the business units concerned. For example, advice should be obtained from independent accountants regarding the information that should be retained for tax purposes. Similarly, attorneys with special expertise in areas such as environmental regulation or export controls should be consulted with respect to the specific record-retention requirements enforced by the applicable federal agencies. Managers in each business unit are also the best source of information on how specific records can be identified and collected, as well as the most effective procedures for storing and retrieving documents. Managers responsible for overseeing the records retention program should become active participants in professional associations of records management administrators in order to gain access to information regarding recognized best practices in this area.

C. Policies and Procedures

The foundation of any records retention program is a formal written records retention policy accompanied by detailed procedures that provide all company employees with instructions on how to create, organize, handle, store and discard business records. There is no standard form of records retention policy; however, it is clear that a well written policy will address the following issues:

- Defining the purpose of the policy and the goals and objectives that the company hopes to obtain by creating and administering the policy.
- Defining the types of records covered by the rules and procedures in the policy, including electronic data.
- Clarifying that all records covered by the policy are the property of the company regardless of where such records were created or stored.
- Establishing the retention period for each type of record in compliance with applicable laws and regulations, including statutes of limitations. This is done through the creation of records retention schedules that become part of the policy.
- Developing procedures for record storage and disposition and establishing a central registry and depository for retained files.
- Establishing procedures for required retention of records in the event that a legal duty to retain and not destroy those records arises due to receipt of a threat of a lawsuit, governmental investigation or audit.
- Compliance with applicable laws and regulations pertaining the storage and preservation of records including conversion of paper records to electronic records.
- Establishing audit procedures and conducting regular reviews to ensure that changes in regulatory requirements and records technology are reflected in the policy (e.g., changes to required retention periods under applicable laws and regulations).
- Establishing procedures for amending and replacing the policy, as well as granting waivers to the application of the policy, and clarifying whether records in existence prior the adoption of the policy are subject to its requirements.

A policy that adequately addresses all of these issues will be an effective tool for ensuring that the company has ready access to all records necessary for it to conduct its business and comply with legal requirements while at the same time lawfully eliminating documents that are no longer needed for operations and which if retained could unnecessarily create liability for the company in future litigation. Once the policy is created, a single person, generally referred to as the records administrator, should be designated to administer the policy and ensure that the procedures included in the policy are being followed and that employees are trained in how to create, preserve, store and catalog, and discard records.

Companies can follow several different formats when drafting their records retention policy. A comprehensive policy would cover each of the topics listed above (*i.e.*,

purpose, types of records, ownership of records, retention periods, storage and disposition procedures, implementation of “litigation holds,” audit procedures and amendments). Another form might focus on the specific requirements that are imposed on departments and business units within the company relating to the management of their records. Some companies adopt a separate policy regarding the retention of records relating to the implementation of the company’s corporate compliance program. Adherence to records retention requirements should also be addressed as part of the company’s broader code of business conduct and ethics.

D. Retention Schedules

Each records retention policy should also include a comprehensive set of records retention schedules that identify all of the legal, fiscal, regulatory and administrative requirements applicable to the company and the record-keeping and retention obligations associated therewith. The records administrator, working with the various departments and business units within the company, should establish guidelines and procedures for determining which categories of records should be included in the records retention schedules and the applicable retention period(s) for each category. The records administrator typically uses just one records retention schedule that includes all of the records categories; however, it is also useful to create separate schedules for different categories of records such as the following:

- General Correspondence and Basic Corporate Records
- Litigation
- Accounting Records and Tax Filings
- Personnel Matters
- Contracts
- Finance
- Acquisitions and Dispositions
- Plant and Property
- Sales, Marketing and Business Development
- Manufacturing
- Products Liability
- Intellectual Property
- Traffic and Transportation
- Security
- Other Regulations
- Records Administration

Some companies create categories within their master records retention schedule that parallel the specific depart-

ments and other business units within the company’s organizational structure. For example, the requirements may be broken out into accounting, personnel, controller’s office, treasury, traffic, sales, imports and exports, corporate administration, research and development, manufacturing and credit. One advantage of this type of system is that provides greater direction as to where particular types of records will actually be stored and administered.

Many records retention periods are actually mandated by statute or regulation; however, if there is no specific statutory or regulatory guideline relating to the retention of a specific record the company should use the time period provided for in the statute of limitations for any legal action in which the document might be relevant. For example, a document used in connection with a registered public offering of securities should be retained for at least three years, which is the time period during which actions must be brought for false or misleading statements contained in a registration statement or prospectus and filed with the Securities and Exchange Commission in accordance with the Securities Act of 1933, the Exchange Act of 1934, and other federal securities laws.

E. Records Retention Manuals

Most companies, regardless of size, will have some form of policy guidelines regarding retention and storage of records. In larger companies, it makes sense to develop a separate manual that includes guidelines and the criteria to be used in deciding which documents should be saved and how long they should be stored. The manual should specify or define what constitutes a corporate record and outline any special corporate ownership rights. In addition, the manual might distinguish between corporate records and any personal records the company policy might allow. The manual should also list the retention periods for each type of document the corporation receives or generates. Additional subjects that should be covered in the manual include the following:

- Definitions of key terms involved in the records administration process;
- Standards and procedures for the administration of the corporate records administration system;
- Criteria for retention of records:
 - What are Vital or Permanent Records (information that would permit operations to continue or resume without dependence on human institutional memories)?
 - What are Special and/or Proprietary Records?
 - Who has Responsibility for the Record Copy?
 - What controls and accountability, if any, are to be imposed on copies of corporate records?
- Methods of storage and protection of records;

- Criteria for moving and transfer of records;
- Criteria and authorization required for public disclosure of corporate records;
- Criteria and methods for destruction of information and materials no longer deemed to be corporate records (how are copies to be accounted for in the destruction process?);
- Procedures for recovering from disasters involving corporate records;
- Recordkeeping of corporate information released outside of corporate control;
- Interaction between records administration and current operations;
- Procedures and timing for audit and review of the corporate records systems; and
- Procedures for files management.

The manual should state what the company policy is with respect to its records. It should explain why corporate personnel should spend their time bothering about preserving and organizing the corporate records. If the corporate records retention manual is company confidential, here is the place to outline that policy. The manual should outline the purpose of the corporate records retention program and the manual itself.

The manual should distinguish between the responsibilities of corporate operational personnel and full-time corporate records retention personnel. Regular employees should be provided with information regarding the company's conventions with respect to creation, organization, use and storage of records, and the manual should make it clear that each employee is responsible for following those guidelines. If possible, the manual should include several examples to illustrate how the guidelines might work in practice. Employees should also be advised that they are expected to participate in regular training sessions and cooperate with records retention personnel during audits of the entire records retention program.

In addition to the complete corporate records retention manual, a company should have a short, simplified overview version which explains the fundamentals of the corporate records retention program to people in the organization who are expected to spend little of their time on records administration issues. The overview version of the manual should include references to the complete manual where further detail on a particular point can be found. Both the overview and complete manual should be written in plain, simple, everyday, non-technical English.

The manual should be reviewed on a regular basis to ensure that the guidelines take into account all types of records created or used by the company as well as new technological trends relating to the storage of information.

Any changes or modifications should be announced to all employees in advance, and an effort should be made to obtain an acknowledgement from each employee that he or she has been notified of the change.

F. Electronic Documents

Companies now generate a substantial amount of information in the form of electronic documents and the records retention policy must clearly and specifically address retention and destruction of e-mail communications and other types of electronic documents. The general rule is that e-mail should initially be treated in the same way as any other form of written record; however, it is reasonable for companies to authorize deletion of electronic records in order to preserve storage space and ensure that its networks continue to run smoothly so long as deletion does not run afoul of legal requirements and does not expose the company to sanctions in the context of a pending lawsuit or governmental investigation. When developing a record retention policy the legal department should consult closely with the experts in the information technology department to establish procedures that will reduce potential liability and ensure that mistakes are not made when litigation is pending or threatened (i.e., continued operation of automatic destruction programs that inadvertently destroy e-mail message that should be retained for production in the lawsuit). In order to justify destruction of relevant documents just prior to the time that it receives notice of a threatened lawsuit or government investigation the company should be able to point to the procedures set forth in a reasonable records retention policy and demonstrate that the destruction occurred in the normal course of administering that policy.

Companies often take advantage of software programs that search for various key words in e-mail databases in order to identify records that should be retained beyond the date set by the company for automatic destruction of e-mail messages. For example, a search may be made for racial content that might later lead to a harassment or discrimination claim. Another scenario is a search for information on patents or other forms of intellectual property that should be incorporated into the company's permanent records and accessible in the event of a future dispute or at the time that someone in the company begins preparation of a patent application. While scientists and engineers should be instructed to preserve these records on their own beyond the automatic destruction date they may neglect to do so. It is important for the company to emphasize that while these records are created by individuals they are company assets that need to be collected and retained in a fashion where they can be accessed and used by all interested employees.

The Sedona Conference, a nonprofit research and educational institute that is dedicated to the advanced study of law and policy in the areas of antitrust, intellectual

property, and complex litigation, has published *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* (Sept. 2004). This publication, which can be downloaded from the organization's Web site, provides a comprehensive and reasonable framework on managing electronic information and responding to production requests for such information in the context of a legal proceeding. The five key points of the Guidelines are as follows:

- An organization should have reasonable policies and procedures for managing its information and records.
- An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.
- An organization need not retain all electronic information ever generated or received.
- An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.
- An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

Commentaries to the Guidelines emphasize the need for reasonableness, practicality and flexibility. For example, it is important to understand and accept that defensible policies need not mandate the retention of all information and documents and that no single standard or model can fully meet an organization's unique needs. Effective information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities. The Guidelines also address one of the most sensitive issues relating to management of electronic records—destruction—and make it clear that destruction is an acceptable stage in the information life cycle and that an organization may reasonably and lawfully destroy or delete electronic information when there is no continuing value or need to retain it. Thus, for example, absent a legal requirement to the contrary, companies may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voicemail, and may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes. Of course, companies must recognize that suspending the normal disposition of electronic information and records may

be necessary in certain circumstances and the Guidelines discuss reasonable steps that can and should be taken in the event it is necessary to implement a "legal hold" upon notice of a prospective legal proceeding. Record management policies should be supported by employee education and periodic compliance reviews. Obviously the retention policy should cover electronic documents on the company's own network; however, it should also be broad enough to cover computing devices that employees might use for work activities outside of the office—laptops, Blackberries and/or computers in their home offices.

G. Checklist

When creating and administering a records retention program, the following checklist may be helpful:

1. Identify the specific purposes to be achieved by creating and administering the records retention program.
2. Identify the specific laws and regulations that pertain to the records created or received by the company and determine the records retention requirements in those laws and regulations.
3. Determine the need to contract with consultants and other experts to establish and maintain the records retention program.
4. Prepare and disseminate a formal written records retention policy accompanied by detailed procedures that provide all employees with instructions on how to create, organize, handle, store and discard business records.
5. Establish the retention period for each type of record in compliance with applicable laws and regulations, including statutes of limitations, by creating records retention schedules.
6. Develop procedures for record storage and disposition and establish a central registry and depository for retained files.
7. Develop procedures for handling and storing electronic records.
8. Designate a records administrator who will be responsible for overseeing the creation and administration of the records retention program and ensure that the program is supported by adequate personnel and financial resources.
9. Conduct regular training programs for all employees relating to creation, organization and handling of records and create and disseminate other educational tools such as records retention manuals.
10. Establish and enforce procedures for creating and administering a "litigation hold" whenever it is necessary to suspend regular records destruction

procedures due to the initiation or threat of litigation and/or governmental investigation.

11. Establish audit procedures and conduct regular reviews to ensure that changes in regulatory requirements and records technology are reflected in the policy (e.g., changes to required retention periods under applicable laws and regulations).

II. Business Considerations

A. Identification and Inventory of Business Records

One of the challenging issues associated with developing a records retention program is that there is no single set of rules and guidelines that can be applied to all types of records generated or received by a company. Separate and different legal requirements will apply to the company's business activities and each department or other business unit within the company will have its own specific concerns. In general, companies tend to categorize their records along departmental or functional lines rather than by broad descriptions of documents or their subject matter. This approach will usually work just fine; however, there will always be records that cannot easily fit within that type of categorization and the records retention policy will include specific guidelines for classes of records that are created and used across business units. In addition, the records retention policy must provide guidance on specific forms of records that can be used by every business unit to create content that is subject to the retention program. E-mail is the most obvious example of this issue and the policy should direct employees as to how electronic records will be managed and retained. Finally, records that employees might otherwise consider to be "personal," such as diaries, calendars and appointment books, should be part of the retention program since they often contain business-related information. Information generated and stored in a home office environment must also be integrated into the program.

There are a number of views on just what constitutes a "record"; however, the correct answer will vary depending on the industry and type and size of business and consultants suggest that the process begin with the definition that is incorporated into the "Business Record Exception" to the Hearsay Rule set out in Section 803(6) of the Federal Rules of Evidence. Admittedly, the exception begins quite broadly by referring to "records of regularly conducted activity," and then provides the following additional explanation:

A memorandum, report, record or data compilation, in any form, of acts, events, conditions, opinions or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course or a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation

This definition clearly covers items that are traditionally understood to be "documents," which include accumulations or compilations of data that are set out in a particular format. An obvious example would be contracts, as well as policies and procedures. In some cases, documents are "controlled" and include a history of all changes that have been made to the document from the time that it was initially created.

It is important to remember, however, that the reference to "records" casts a much more comprehensive net and may include computer records, including electronic logs, and information that resides on the company's hard drives and other media that may become a repository of information. For example, companies that make extensive use of computerized data and other sources of electronic information should expect to have their policies cover such things as voice mail messages and files, back-up voice mail files, e-mail messages and files, back-up e-mail files, deleted e-mails, data files, program files, back-up and archival tapes, temporary files, system history files, website information stored in textual, graphical or audit format, cache files, cookies and other electronically recorded information. Another potential problem is the need to search for records on portable devices, such as laptop computers, PDAs and cell phones, and to make sure that notice is taken of records that may exist outside of the company's offices, including the personal computers of employees allowed to work at home.

Once the definition of "records" has been finalized, the next step in the process is to create a comprehensive inventory of all the records that may be created by users in all departments and at all locations within the company. While creating the inventory, the records should be placed into identifiable and meaningful categories that correspond to the functional purposes and uses of the records included within such categories. This rule should be followed for all types of records, not just those that exist in the traditional paper format. For example, companies should inform all of their employees to treat electronic communications, such as e-mail, and files on their computers in the same way as they deal with paper documents. Employees should be trained on the proper way to store and organize e-mail messages; and, if possible, a standard system should be used throughout the company so that the company can quickly and easily respond to a request for information on a specific subject or transaction. In fact, making sure that electronic documents relating to a particular subject or issue are properly indexed and separated can reduce the risk that counsel for a company competitor or government regulators will be allowed full access to the company's computer records, including information that is totally unrelated to the particular dispute or investigation.

Ideally the records retention program will be broad enough to cover all of the records generated or received by the company; however, in the early stages of implementing

the program the records administrator and the legal department may need to maximize their scarce resources and focus on a few key areas to make sure that the company is properly managing vital records, documents and records obtained from third parties under a specific duty of protection, and electronic records (e.g., e-mail communications). Managers in each department should be asked to identify records that they believe would be absolutely essential for the department to continue operating. This should include important contracts, customer and client lists, product designs, and records required for prosecuting insurance claims. These records should be copied and stored off-site in a secure location.

B. Retention Periods

Once the initial identification and inventory of records is completed, a retention period should be established for each category of records and included in the records retention policy in the form of a records retention schedule. The retention periods are determined by several factors:

- Companies must obviously adhere to specific record retention obligations included in applicable federal, state and local statutes and regulations and these requirements must be reviewed regularly in order to identify amendments.
- Companies must attempt to identify and retain all records that may be relevant in prosecuting or defending potential causes of action in future lawsuits. This is obviously a challenging exercise given that it is impossible to tell with certainty whether or not a particular contract or business relationship will lead to litigation. At a minimum the company should identify all of the potential states in which it is amendable to suit, identify the potential causes of action (e.g., contract, products liability, fraud etc.) and then identify the applicable statutes of limitations which can then be incorporated into the retention periods for specific records. Since statutes of limitations may vary the retention period should be the same as the longest statute of limitation for a particular category of records. As with statutes and regulations it will be necessary to periodically review the statutes of limitations to identify any changes.
- The company should be mindful of how expanding business activities into a new jurisdiction will increase the scope of its records retention responsibilities.
- The company must do a realistic assessment of the materiality of specific records and the likelihood that the company will actually need to refer to a particular record in the future.

In many cases the liabilities associated with a particular record will be outweighed by the expense and inconvenience of storing the record. For example, a company can reasonably decide that it makes little or no sense to keep

records relating to a particular written contract for 15 or 20 years because that is the statute of limitation for contract action if the contract itself is immaterial in relation to the company's business and it is unlikely that the company would get involved in formal litigation over a dispute that might arise over the subject matter of the contract.

With respect to records that are created solely or primarily for regulatory compliance purposes, the minimum retention period must, of course, be the amount of time mandated by the applicable law or regulation. In those cases where a record is created and maintained for more than a single regulatory requirement, the longer required period should govern. A retention period based on actual regulatory requirements should be considered to be the minimum period for retention, and companies should consider the end of that period to be the first date that destruction may be considered rather than the date that the document must be destroyed.

With respect to records that are created other than solely or primarily for regulatory compliance purposes, it is important to establish a retention period that will be viewed to be reasonable considering the facts and circumstances surrounding the documents. In fact, this test should be applied to all records since retention of a record only for the minimum period specified by statute may ultimately be deemed to be unreasonable if it could be foreseen that the records may become material at some point beyond the end of the minimum period. Factors that should be taken into account in determining whether records should be retained beyond the minimum period specified by statute include the following:

- The frequency and likelihood of disputes, including formal litigation, regarding the subject matter of the record. For example, it would appear that written customer complaints should be kept longer than relatively uncontroversial items such as appointment books.
- The ongoing need to consult the records for routine business purposes or to review the historical background for a current project or transaction.
- The need to maintain such records for internal audit requirements, particularly records that are useful in evaluating historical performance.

With respect to documents that might be the subject of litigation or government investigation, reference should be made to the applicable statute of limitations that might be applied by a court or law enforcement entity. In any case, whenever a decision is made to extend or shorten the retention period, due consideration should be given to the risks associated with varying from a period otherwise prescribed by law, and the reasoning behind the decision should be documented and retained.

C. Storage and Retrieval

It is important to ensure that the records retention program integrates strategies and tools for proper storage of the records. The key considerations with respect to storage are organization, accessibility, and security. Records must be easily available for consultation in day-to-day activities and it also must be easy for counsel to access and retrieve older records in order to determine if they include information that must be produced in a lawsuit or a government investigation. An organized and accessible collection of records also facilitates regular destruction of records as they reach the end of their specified retention period. If records cannot be easily located it is quite possible they will be kept much longer than necessary and thus become a significant potential source of legal risk.

The first step with respect to “organization” is selecting and implementing an appropriate system for filing and cataloging the various records generated and received by the company. The key is to make sure that all records can be quickly located and accessed for use in day-to-day activities and to be sure that obsolete records are discarded on the date their retention period ends and not kept in the system to increase storage costs and potential legal exposure. The organization system should be easy to understand and should be described to all employees in manuals and training sessions. The organization system should be supported by adequate storage facilities and products and a trained administrator should be available at all times to assist employees with questions about how records should be categorized and stored. The organization system should be regularly inspected and audited to ensure that records are, in fact, being placed in the appropriate locations. The issue of “accessibility” is closely related to organization and specifically addresses the issue of making sure that all records can be readily located. Success in this area is measured by how efficiently information can be accessed for day-to-day activities and through audits that focus on the likelihood that a specific record is where it should be under the program’s systems and procedures. Records should be searchable based on several characteristics including topic and date. The program should include procedures for transferring and tracking possession of records.

When determining the best way to store records, consideration must also be given to establishing the appropriate level of security for sensitive records and making sure that records are stored in a way that they can be reliably preserved regardless of the occurrence of natural disasters and other events that might cause unintended destruction of records. Special attention should be paid to critical and confidential records that cannot be replaced and/or the loss of which may create substantial liabilities for the company. Examples include corporate records, trade secrets, records of financial transactions, personnel files and other employee records, insurance records, and records that must be safely preserved pursuant to governmental requirements. The

records retention administrator should work closely with the legal department to ensure that all sensitive records are appropriately marked as “confidential” and that access to those records is restricted. Access procedures should also take into account federal and state privacy laws. Reliable preservation can be achieved by making sure that records are stored in the proper environmental conditions and that steps are taken to protect records against fire and water damage. In most cases companies arrange for copies of particularly important records to be stored in an off-site facility. This includes co-location of company services with an outside service provider.

Electronic records storage is obviously important when there is a threatened lawsuit or government investigation since the company will be required to take necessary steps to preserve electronic communications and other records that might be subject to production. Apart from that scenario, however, companies may store electronic versions of records (e.g., contracts) and should be sure that this is done in a way that conforms to the electronic records standards that might be established by the applicable governmental agency such as the Internal Revenue Service or the Securities and Exchange Commission. Contracts entered into electronically should be “documented” through electronic records that conform to statutory requirements such as the applicable version of the Uniform Electronic Transactions Act.

D. Records Destruction

One of the goals of the records retention program is to establish the appropriate “lifecycle” for each record and ensure that the record is destroyed once it is no longer needed and retention is not mandated by any particular statutory or regulatory requirement. Accordingly, once the record retention periods have been established, policies and procedures should be implemented to regulate the actual destruction of the records. The basic principle is that the records retention program should provide for regular, systematic reviews of the contents of all files to determine the age of particular records and removal of those records that need not be retained. When pulling records for destruction, consideration must be given to the fact that there may be duplicate copies and it is important for all copies of an obsolete document to be located and destroyed. This includes personal copies that may have been retained by employees involved with a transaction during which the record was generated as well as backup copies that may have been moved to an off-site storage facility.

All records that have been identified for disposal should be carefully handled and it is useful to keep the following suggestions in mind:

- Maintain a log or other record of the title and dates of records to be destroyed. This can be an annotated version of an existing inventory on file.

- Oversee and sign off on the destruction. The records administrator should be notified before any records are destroyed and should take responsibility for overseeing the entire process.
- Verify labels and contents by checking inside boxes. Do not assume that the label is correct or inclusive (folders are often reused). Obliterate old labels before recycling boxes.
- Destroy the record in a manner that is appropriate to the level of confidentiality of the information. Most records can be recycled or placed in landfill, but documentation such as payroll and donor information may need to be shredded.
- Modify the records retention schedule by following a formal process. Bring proposed retention policies before appropriate parish committees and officers to receive approval for changes.

Document destruction procedures should be consistently followed with the only exception being cases where there is an existing or threatened government investigation or lawsuit. The records administrator, the legal department, and the information systems department should work closely to establish procedures for alerting all impacted employees as soon as the company is made aware of the possibility of an investigation or lawsuit and formal notices should be disseminated regarding suspension of routine records destruction programs. While this seems straightforward on its face, companies must guard against the possibility that records may be destroyed during a period in which such records may be necessary for presentation in litigation or an investigation launched by a law enforcement agency. One procedure that must be implemented is a comprehensive and reliable method of informing all relevant managers and employees of the need to suspend document destruction that might otherwise be undertaken under the company's normal record destruction procedures. In addition, companies should consider notifying senior managers in advance of any proposed document destruction so that consideration can be given to whether such destruction should or must be delayed. In any case, development and enforcement of these policies should not be left to persons at lower levels of the company since courts have placed responsibility for preservation of potentially discoverable material on the shoulders of senior corporate officers.

While destruction procedures should be continuously followed and exceptions made only after careful consideration it is important for the records administrator to take into account the interest of the company in identifying and preserving its historical resources. Every company generates or receives records that should be maintained in perpetuity because of their enduring value to the company and the records administrator should establish a separate definition of what might be deemed a "permanent record"

of the company. Several factors should be taken into accounting include administrative value (e.g., building plans and annual reports), fiscal value (e.g., property inventories), historical value (e.g., artifacts) and legal value (e.g., meeting minutes, correspondence). Records designated as "permanent" should be transferred to a safe and proper location designated as the company archives where they can be protected and made available for appropriate use and review.

E. Staffing and Accountability

Records retention is an important program and companies should be sure that the project is adequately staffed and that is clear which person or persons are to be held accountable for making sure that a record can be located and that destruction procedures are followed. For smaller companies, one person should be designated as the first source for locating records. The person should be familiar with all applicable legal and business requirements and should understand how records are organized and used in day-to-day operations. Larger firms may have several people assigned to the program; however, it is important for one person to have final responsibility. The staff, however large, should be assisted by software programs and other tools that can be used to track the location of records and automate the initial inventory process.

Given the sheer number of records that a company will generate during the course of its day-to-day business it is not surprising that creating and administering a records retention policy can be an extremely challenging project. There are, however, a wide range of resources and technological tools available for records managers and administrators. For example, consideration should be given to contacting and joining the Association of Records Managers and Administrators, which is a group of professional records managers and administrators that has local chapters in many major cities. Among other things, this organization publishes a journal on records management issues, disseminates technical publications, and conducts workshops on records management topics. Companies may also use outside consultants to assist with the development of a records retention program; however, a consulting arrangement should not be used unless and until there is a clear understanding regarding the amount of time that the consultant is expected to spend on the project and the fees that will be charged for completing the work. One obvious problem with using an outside consultant is that the consultant will not know the company and may need to spend a substantial amount of time learning about the company's business and workflow. Finally, there are a number of vendors ready to sell records retention tools including files, filing cabinets, offsite storage facilities, and software programs to organize information regarding the company's inventory of retained records.

Records Retention: Part II*

by Alan Gutterman**

ISSUE NO. 131
November 2008

* This material was reprinted from *Business Transactions Solutions* (available as a Westlaw database, BTS) with permission from the author.

** Alan Gutterman is a partner at the San Francisco and Silicon Valley offices of *The General Counsel* (<http://www.thegeneralcounsel.net/>), a provider of interim in-house general counsel and attorney recruitment services. Mr. Gutterman has over two decades of experience as a partner and senior counsel with internationally recognized law firms counseling small and large business enterprises in the areas of general corporate and securities matters, venture capital, mergers and acquisitions, international law and transactions, strategic business alliances, technology transfers and intellectual property, and has also held senior management positions with several technology-based businesses. Mr. Gutterman is also the author of several publications, including *Business Transactions Solutions*, *California Transactions Forms*, *Corporate Counsel's Guide to Strategic Alliances*, and *Corporate Counsel's Guide to Technology Management and Transactions*.

Note: This is the second in a two-part article discussing general procedures for establishing and administering a records retention program. Part I appeared in last month's issue of this newsletter, and covered practice and business considerations of a records retention program. In Part II below, legal and tax considerations are discussed and checklists for drafting and reviewing records retention policies are included.

III. Legal Considerations

A. Records Retention Requirements

The record retention requirements applicable to a corporation under statutes

continued on page 2

Letter from the Editor.....1

Records Retention: Part II.....1

III. Legal Considerations1

IV. Tax Considerations.....6

V. Drafting Checklist:
Comprehensive Records
Retention Policy6

VI. Review Checklist:
Comprehensive Records
Retention Policy7

Dear Subscribers:

In this issue of Corporate Counsel's Records Retention Report, we are pleased to provide the second part of a two-part article written by Alan Gutterman. The first part of this article appeared in last month's issue of this newsletter. The article generally discusses procedures for establishing and administering a records retention program. Part I covered practice and business considerations. This second part discusses legal and tax considerations, including employment and securities laws, the Consumer Product Safety Act, international considerations, electronic document discovery rules, as well as drafting and review checklists. Again, our thanks to Mr. Gutterman for allowing us to share his article with our subscribers.

Very truly yours,
Jeanne D. Wertz
Senior Attorney Editor

and regulations are extensive and disbursed throughout the Code of Federal Regulations (C.F.R.). In fact, the C.F.R. index has over 1500 references to reporting and record keeping requirements including general requirements that would apply to almost all companies doing business (*e.g.*, employment and tax records) and additional requirements that apply to specific types of businesses. Fortunately, there are a number of commercial resources available for streamlining the process of determining the records retention requirements that might apply under federal statutes and regulations. A good starting point for more detailed research would be *The Guide to Record Retention Requirements in the Code of Federal Regulations*, which is a compendium of the federal record keeping provisions prescribed by various federal departments or agencies in the C.F.R. Unfortunately, although not surprisingly, knowledge of the federal requirements is not sufficient particularly since some states have reporting requirements in particular legal areas that exceed the federal requirements. This means that companies that are considered to be “doing business” in those states will be subject to additional record retention obligations. Fortunately many states have prepared publications that describe the record retention requirements under their own statutes and regulations. Professional service providers in particular business areas also publish a summary of relevant records retention requirements. For example, human resources consultants can provide information on how long records should be maintained in order to comply with federal employment laws and regulations and accounting firms readily disseminate schedules showing how long tax and accounting records should be kept.

The array of federal statutes and regulations that must be considered when creating and managing a records retention program can be overwhelming. Some statutes and regulations generally apply to all types of businesses; however, the actual scope of a company’s obligations depends on its specific business activities (*i.e.*, industries, location, customers, types of assets etc.). An extensive, although by no means all-inclusive, list of the types of federal statutes and regulations that need to be considered includes the following:

- Federal employment laws, including the Age Discrimination in Employment Act, Title VII of the Civil Rights Act of 1964, the Fair Labor Standards

Act, the National Labor Relations Act, the Employee Retirement Income Security Act of 1974, the Occupational Safety and Health Act, the Americans with Disabilities Act and the Family and Medical Leave Act of 1993.

- The antitrust laws, including the need to maintain records necessary to support the applicability of the cost-justification and/or meeting competition defenses under the Robinson-Patman Act.
- Federal securities laws, including specific requirements for broker-dealers.
- Laws and regulations pertaining to consumer protection, including the Consumer Product Safety Act and the Magnuson-Moss Warranty Act.
- Laws and regulations pertaining to international business activities, including import and export activities and engagement of foreign agents and business partners.
- Laws and regulations pertaining to government contracts and independent contractors.

1. Employment Laws

Every business, regardless of its size, must keep accurate and complete records regarding its employees from the date of the employee’s application for employment through the employee’s termination and thereafter for at least the applicable statute of limitations period. Among other things, companies must maintain information and records for each employee regarding wages and payment practices, benefits, employment agreements and other terms of employment, vacation and leaves of absence, personnel actions, collective bargaining agreements, references, health and safety, drug and alcohol testing, and records relating to certain demographic criteria (*e.g.*, race, sex and national origin) as required under laws prohibiting discriminatory practices.

2. Securities Laws

In addition, the SEC has established specific records retention periods for various industries, such as public utility holding companies. 17 C.F.R. § 257.2. In addition, the SEC enforces books and records requirements for specific types of companies and transactions. For example,

Copyright 2008 Thomson Reuters/West. All rights reserved. *CORPORATE COUNSEL’S RECORDS RETENTION REPORT* (ISSN 1098-0261) is published monthly by Thomson Reuters/West, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Subscription Price: \$210.00 annually. *This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice. If legal advice or other expert assistance is required, the service of a competent professional should be sought.* The information contained herein is based upon sources believed to be accurate and reliable—including secondary sources. Where cases, statutes, or other official materials have been reprinted, we have attempted to provide materials as close to the originals as possible, but we do not purport to publish any documents verbatim. While we have exercised reasonable care to ensure the accuracy of the information presented, no representation or warranty is made as to such accuracy. Readers should check primary sources where appropriate and use the traditional legal research techniques to make sure that the information has not been affected or changed by recent developments.

the SEC's rule under the Commodity Exchange Act provides that: "[a]ll books and records required to be kept by the [Commodity Exchange] Act or by these regulations shall be kept for a period of five years from the date thereof and shall be readily accessible during the first two years of the five-year period. All such books and records shall be open to inspection by any representative of the [SEC] or the United States Department of Justice" 17 C.F.R. § 1.31(a)(1).

As a general rule, companies must maintain a copy of all materials filed with the SEC pursuant to Securities Act and Exchange Act disclosure requirements for at least five years. For example, the SEC rules relating to Securities Act filings provides: "Where the [1933] Act or the rules thereunder ... require a document filed with or furnished to the [SEC] to be signed, such document shall be manually signed, or signed using either typed signatures or duplicated or facsimile versions of manual signatures. ... Such document shall be executed before or at the time the filing is made and shall be retained by the registrant for a period of five years. Upon request, the registrant shall furnish to the [SEC] or its staff a copy of any or all documents retained pursuant to this section." 17 C.F.R. § 230.402(e). With respect to the Exchange Act, the general rule is as follows: "Where the [1934] Act or the rules, forms, reports, or schedules thereunder ... require a document filed with or furnished to the [SEC] to be signed, such document shall be manually signed, or signed using either typed signatures or duplicated or facsimile versions of manual signatures. ... Such document shall be executed before or at the time the filing is made and shall be retained by the filer for a period of five years." 17 C.F.R. § 240.12b-11(d). The five-year requirement applies to shareholder documents filed with the SEC under the Exchange Act, 17 C.F.R. § 240.14d-1(h) (stating that these documents "shall be executed before or at the time the filing is made and shall be retained by the filer for a period of five years.") and to Section 16 reports (*i.e.*, Forms 3, 4, and 5) 17 C.F.R. § 240.16a-3(i).

3. Consumer Product Safety Act

The Consumer Product Safety Act (CPSA) provides that "[e]very person who is a manufacturer, private labeler, or distributor of a consumer product shall establish and maintain such records, make such reports, and provide such information as the Commission may, by rule, reasonably require for the purposes of implementing this chapter, or to determine compliance with rules or orders prescribed under this chapter." 15 U.S.C.A. § 2065(b). The stated obligations are quite broad and reference can and should be made to implementing regulations for the CPSA which do include specific provisions regarding retention periods for particular products. As to those products not covered by specific rules the manufacturer, private labeler or distributor is left at sea as to what types of records would be required and how long they should be kept; however, since the concern of the regulating body is manufacturing,

testing, sale or distribution it should be expected that the document relating to injuries caused by any product or product malfunctions should be retained (*i.e.*, consumer claims and complaints, test reports, investigative reports, or engineering records).

4. International Business Operations

Companies engaged in business operations outside of the United States will need to establish and maintain a compliance program that ensures that the company satisfies the requirements of various laws and regulations pertaining to import and export activities and the engagement of sales representatives and other business partners in foreign countries. Most of these laws and regulations include their own separate records retention requirements. For example, the records and accounting section of the Foreign Corrupt Practices Act requires any company that has stock registered with the SEC to make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets of the company; and devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:

- All transactions are executed in accordance with management's general or specific authorization;
- Transactions are recorded as necessary to permit preparation of financial statements in conformity with generally accepted accounting principles and to maintain accountability for assets;
- Access to assets is permitted only in accordance with management's general or specific authorization; and
- The recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.

B. Electronic Document Discovery Rules

When the widely anticipated and discussed amendments to the Federal Rules of Civil Procedure dealing with electronic evidence finally came into effect on December 1, 2006, companies were formally put on notice that they would need to carefully evaluate their records retention policies to ensure that they would be able to comply with discovery requests. While the changes only apply to federal courts, it is certain that similar modifications will be made to the rules governing discovery practice in state courts.

The amendments focus on how parties to litigation should deal with electronically stored information, a concept that includes the vast array of information and data that may reside on computers, disks, tapes, electronic devices and the Internet. The notion that electronically stored information is evidence is nothing new; however, one

of the principles behind the amendments was to make it clear that electronically stored information is discoverable and that requests for documents in the discovery process should be understood to include such information as well as the paper-based documents that have been the traditional foundation for production and review. As a result, document retention and preservation policies must now be expanded, if they have not been already, to include any medium where electronic information might be stored including spreadsheets, databases, voice messaging systems and the like. Moreover, given that this type of information is often stored by third-party custodians, such as outside accountants and application service providers, companies must be more vigilant about overseeing how those parties preserve and protect information that may ultimately become the subject of a discovery request.

The amendments make it clear that parties must disclose electronically stored information as well as documents that they may seek to use as support for their claims or defenses. Specifically, the parties must provide one another with a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party. Electronically stored information is understood to include writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained. F.R.C.P. Rule 26(a)(1)(B), F.R.C.P. Rule 34(a).

Discovery of some electronically stored information raises very difficult and challenging issues with respect to the nuts-and-bolts of locating, retrieving and actually providing such information to the requesting party. While electronic storage systems often make it easier to locate and retrieve information, some sources of electronically stored information can be accessed only with substantial burden and cost. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. The responding party must identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing and should provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.

If the requesting party brings a motion to compel discovery or for a protective order with respect to such information, the party from whom discovery is sought bears the burden of showing that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery. F.R.C.P. Rules 26(b)(2)(B). It is hoped that, before a court

is asked to order discovery, the parties would meet to discuss the burdens and costs associated with accessing and retrieving the information, the needs of the requesting party that may be asserted to establish “good cause,” and any conditions that may be agreeable to both parties with respect to obtaining and producing the information.

The parties to the litigation must discuss discovery of electronically stored information, including any issues relating to the form or forms in which it should be produced, during the initial “meet and confer” process if such discovery is contemplated in the action and must provide to the court a report regarding the results of the discussion. F.R.C.P. Rule 26(f)(3), F.R.C.P. Rule 35. In addition, the parties must include in their discovery plan any proposal that they might have for the court to enter a case-management or other order adopting such an agreement. It is hoped and anticipated that this will provide an opportunity for the court to get involved early in the litigation process to identify and resolve potential difficulties that might arise with respect to discovery of electronically stored information. Since the issues relating to discovery of electronically stored information will vary depending on the parties’ information systems, the parties are to be familiar with, and prepared to discuss, those systems at the time the conference occurs. This will enable the parties to develop a reasonable discovery plan that takes into account system capabilities. If necessary, the parties should consider open discovery by calling on individuals with special knowledge of a party’s computer systems to provide information that can be used to develop the discovery plan. If possible, the parties should attempt to reach agreement regarding the forms of production for electronically stored information so that future disputes are minimized and the discovery process is more efficient and less costly.

Preservation of discoverable information, including electronically stored information, must also be discussed during the initial “meet and confer” process. F.R.C.P. Rule 26(f). This is a particular concern given that the ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Accordingly, it is essential to deal with preservation of electronically stored information as soon as possible to avoid disputes over whether certain information was intentionally deleted or lost under circumstances where it would have been reasonable for the party to take steps to prevent the loss once the party became aware of the possibility that the information would need to be produced. As with other issues in this area, the scope of preservation requires a balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. In general, it would be unreasonable to ask a party to completely freeze all of its routine computer operations since this could be terribly disruptive to the business and also quite expensive. Courts are reluctant to get deeply involving in preservation, and it is

not intended that courts should routinely issue preservation orders. The hope is that the parties to litigation will use the “meet and confer” process as a way to reach voluntary agreement on preservation measures that are reasonable. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system. Routine operation would include alteration and overwriting of information, which often occurs without the operator being aware of the action or providing any specific direction for the action to be taken. F.R.C.P. Rule 37(f). It should be noted, however, that most commentators believe that, in order for parties to take advantage of the “good faith” safe harbor, they will need to demonstrate that their overall preservation efforts were reasonable and timely.

Electronically stored information raises unique privilege issues that should also be discussed during the “meet and confer” process. Regardless of whether the discovery relates to traditional paper documents or electronically stored information, it is now commonplace for parties to spend substantial amounts of time and money reviewing materials that have been requested during the discovery process to determine whether steps need to be taken to avoid waiver of privilege. The task becomes even more difficult with electronically stored information given the volume of material that would need to be examined and relative lack of formality associated with e-mail and other forms of electronic communications. Another concern is that potentially privileged information may appear in “embedded data” retained on computer programs including draft language and editorial comments. To minimize costs and delays associated with waiver of privilege concerns, it is recommended that the parties work to limit the scope of the materials that need to be produced so that the responding party can focus its waiver review on a finite universe of information. One commonly used method, referred to as a “quick peek,” allows the responding party to provide certain requested materials for initial examination without waiving any privilege or protection. Based on that review, the requesting party then provides a list of the documents that should be formally produced, and these are the documents that the responding party will carefully review to determine whether it wishes to assert any privilege claims.

It is reasonable for parties to litigation to be concerned about potential burdens on third parties as a result of subpoenas that may be served on such third parties to provide information that might be relevant to the litigation. It is clear that electronically stored information can be sought by subpoena and that the subpoena can designate a form or forms for production of electronic data. F.R.C.P. Rule 45(a)(1). Of course, a person served with such a subpoena has the right to object to the requested form or forms. F.R.C.P. Rule 45(c)(2). When a party is advised of actual or potential litigation and considers the scope of

its “litigation hold” instructions, it should include third parties that are subject to its direction and control and that store electronic information that might be relevant to the litigation. Once a subpoena is served on a third party, it should be mindful of protections available to it to avoid undue impositions on nonparties. The general rule is that any party serving a subpoena “shall take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena.” F.R.C.P. Rule 45(c)(1). Nonparties have the right to object to a subpoena, and any court order that requires compliance with a subpoena must also protect a person who is neither a party nor a party’s officer from significant expense resulting from compliance. F.R.C.P. Rule 45(c)(2)(B).

C. Potential Liabilities

Companies that fail to establish and maintain record retention programs and violate their statutory and regulatory obligations with respect to reporting and record-keeping risk substantial liability including fines and adverse judgments in civil litigation. The explosion in the importance and volume of electronic documents has created additional potential problems in the form of sanctions for failure to preserve and produce information that is included in e-mail communications. Each federal regulatory agency responsible for promulgating regulations pertaining to retention of records has the authority to enforce those requirements and companies should be mindful of the specific practices of each agency that has oversight power over their business activities. In general, regulatory agencies have the right to enter the facilities of a company and inspect the company’s books and records. In addition to civil fines, companies found to be engaged in willful violations of federal record keeping requirements may be prosecuted under various criminal statutes including conspiracy and obstruction of proceedings and may be subject to sanctions prescribed under the Federal Sentencing Guidelines.

Of course, companies must also be mindful of potential liabilities for violating state laws relating to reporting and retention of records. As is the case at the federal law, state regulatory agencies have the responsibility for enforcing the record-keeping requirements included in the statutes that they oversee and they also have the right and discretion to engage the office of the state attorney general to launch a criminal investigation and prosecution when companies fail to properly maintain records or engage in destruction of records in order to avoid prosecution under state laws and regulations.

In addition to the civil and criminal penalties that may be imposed on companies that breach federal and state statutes and regulations pertaining to records retention they stand to suffer in a number of other ways. First of all, it is costly and time-consuming to mount a defense against a government agency that is claiming that records have not been maintained or readily made available as required by

law or statute. Second, this type of problem generally is perceived very negatively within the company and among the company's business partners and can significantly harm the company's reputation.

It is also important to remember the impact that records retention might have on the outcome of civil litigation. For example, the ability of a company to prosecute a claim or assert a defense in a lawsuit may turn on whether or not it can locate and produce the appropriate documentation. In fact, before deciding if a lawsuit should be filed the company should review its own records to be certain that it has sufficient documentation to support any affirmative claims it wishes to make against the proposed defendants. On the other hand, there is the risk that records that are retained in accordance with the records retention policy may contain information that can be used against the company in litigation. Unfortunately, while this may happen it is not a reason for a company to engage in willful activities to violate statutory records retention requirements.

IV. Tax Considerations

The federal tax laws, and the Internal Revenue Service, generally provide the clearest and most complete answer to the question of what records need to be retained by individual and corporate taxpayers and the length of the retention periods. The general record-keeping requirements relating to tax records are found at 26 U.S.C.A. § 6001, which in part provides as follows: "Every person liable for any tax ... shall keep such records, render such statements, make such returns, and comply with such rules and regulations as the [IRS] may from time to time prescribe." The IRS has promulgated lengthy regulations to clarify the statutory requirements. The general rule and principle is that "[a]ny person required to file a return of information with respect to income, shall keep such permanent books of account or records, including inventories, as are sufficient to establish the amount of gross income, deductions, credits, or other matters required to be shown by such person in any return of such tax or information." See 26 C.F.R. § 1.6001-1. The term "permanent," as used in the regulations, does not mean that the relevant records must be retained indefinitely. It only refers to the permanence of the method by which the records are kept. It should be noted that taxpayers need not keep every record that is possibly related to determination of tax liability. Instead the taxpayer should limit its retention activities that are "material" 26 C.F.R. § 1.6001-1(e) (records should be retained "so long as the contents thereof may become material in the administration of any internal revenue law"). The general rule is that "material" tax-related records should be kept for at least as long as applicable statute of limitations under the Internal Revenue Code runs; however, taxpayers may be required to keep records longer than that in the case of extension and when issues of fraud have been raised. The IRS does require permanent retention of records in certain cases.

V. Drafting Checklist: Comprehensive Records Retention Policy

The following checklist enumerates information that should be collected to draft a comprehensive records retention policy.

1. Purpose and Scope

1.1 Define the purpose of the policy and describe the goals and objectives that the company hopes to obtain by creating and administering the policy. The main objectives of any records retention policy are compliance with applicable laws and regulations; ensuring that all necessary records remain accessible for as long as those records are required for legal purposes and for legitimate business needs; managing and reducing the costs associated with records retention activities; and making sure that all records necessary for the company to fulfill its reporting and accounting obligations to taxing authorities are available for the minimum periods specified in the tax laws.

1.2 Define the types of records covered by the rules and procedures in the policy, including electronic data. In general, the intended scope of the policy will include all the paper and electronic records of the company including, without limitation, e-mail messages, instant messages, memos, letters, and written agreements. It is important to periodically consider how new communications technologies may have impacted the way in which persons exchange and store information and the policy should be broad enough to incorporate those types of changes.

1.3 Include a statement that clarifies that all records covered by the policy are the property of the company regardless of where such records were created or stored. For example, a document received by an employee relating to his or her business activities that the employee is keeping in a home office will nonetheless be considered a company-owned record regardless of the fact that it is not located in a building owned or leased by the company.

2. Retention and Destruction of Records

2.1 Establish the retention period for each type of record in compliance with applicable laws and regulations, including statutes of limitations. The retention period is determined by several factors—how long the particular record will be needed in order for the company to conduct its business activities and how long the record will need to be retained in order to meet the minimum retention requirements that may be established as a matter of law. Legal requirements can be further broken down into explicit record-keeping requirements that have been included in statutes and regulations and the statutes of limitations that may apply to potential legal actions in which the records might be relevant.

2.2 Prepare a comprehensive records retention schedule that lists each of the categories of records generated or

received by the company and the applicable retention periods for each of the records categories. The schedule should include descriptors such as record series title, description, retention periods, and special notes on handling of certain records.

2.3 Establish procedures for record storage and disposition and establish a central registry and depository for retained files. The policy must provide for prompt purging and destruction, on a regular basis, of records that have completed their respect retention periods.

2.4 Establish procedures for required retention of records in the event that a legal duty to retain and not destroy those records arises due to receipt of a threat of a lawsuit, governmental investigation or audit (not in the ordinary course of the company's scheduled financial reporting) involving the company. Suspension of records destruction in these instances is referred to as a "litigation hold" and should be handled carefully, particularly in the case of electronic records such as e-mail messages.

2.5 Ensure that the policy complies with applicable laws and regulations pertaining the storage and preservation of records including conversion of paper records to electronic records. The administrator should consult with legal counsel before proceeding in order to make sure that all applicable legal requirements have been satisfied. Examples include rules promulgated by the Internal Revenue Service regarding the use of automatic data processing systems to store transactional records that may be subject to audit in the future.

3. Administration and Audit

3.1 Assign responsibility for creating, administering, auditing and amending the policy. This type of policy is typically overseen by a "records administrator" appointed by senior management who is responsible, with his or her staff, for establishing a framework for categorizing information, setting up systems to track where records are located at any point in time, auditing compliance with the policy, making sure that records are promptly purged when they have reached the end of their designated retention period, amending the plan to take into account changes in technology and the company's business activities, and training employees on how to create and store records.

3.2 Establish audit procedures and provide for the conduct of regular reviews to ensure that changes in regulatory requirements and records technology are reflected in the policy (e.g., changes to required retention periods under applicable laws and regulations).

3.3 Establish procedures for conducting a company-wide review of all records that have not yet been moved to a central storage capability to determine whether such records can and should be moved to the storage capability or purged and destroyed as no longer being necessary under the applicable records retention schedule. The

records administrator should develop checklists that can be consulted when auditing the records created or received by particular employee including reminders about the types of records they might have and where they might be stored.

3.4 Establish procedures for amending and replacing the policy, as well as granting waivers to the application of the policy, and clarifying whether records in existence prior the adoption of the policy are subject to its requirements. For example, if the company becomes involved in new business activities it will likely become subject to a host of different statutes and regulations that have their own unique records retention requirements and it will thus be necessary to make amendment to the existing policies and procedures.

4. Client and Transaction Information

4.1 Name of Client: [name]

4.2 Client Contact: [name]

4.3 Date of Interview: [date]

4.4 Opposite Parties: [name(s)]

4.5 Other: [description]

VI. Review Checklist: Comprehensive Records Retention Policy

The following checklist enumerates issues that should be considered when reviewing a comprehensive records retention policy.

1. Purpose and Scope

1.1 Does the policy include a definition of its purpose and describe the goals and objectives that the company hopes to obtain by creating and administering the policy? The main objectives of any records retention policy are compliance with applicable laws and regulations; ensuring that all necessary records remain accessible for as long as those records are required for legal purposes and for legitimate business needs; managing and reducing the costs associated with records retention activities; and making sure that all records necessary for the company to fulfill its reporting and accounting obligations to taxing authorities are available for the minimum periods specified in the tax laws.

1.2 Does the policy define the types of records covered by the rules and procedures in the policy, including electronic data? In general the intended scope of the policy will include all the paper and electronic records of the company including, without limitation, e-mail messages, instant messages, memos, letters and written agreements. It is important to periodically consider how new communications technologies may have impacted the way in which persons exchange and store information and the policy should be broad enough to incorporate those types of changes.

1.3 Does the policy clarify that all records covered by the policy are the property of the company regardless of where such records were created or stored? For example, a document received by an employee relating to his or her business activities that the employee is keeping in a home office will nonetheless be considered a company-owned record regardless of the fact that it is not located in a building owned or leased by the company.

2. Retention and Destruction of Records

2.1 Does the policy establish the retention period for each type of record in compliance with applicable laws and regulations, including statutes of limitations? The retention period is determined by several factors—how long the particular record will be needed in order for the company to conduct its business activities and how long the record will need to be retained in order to meet the minimum retention requirements that may be established as a matter of law. Legal requirements can be further broken down into explicit record-keeping requirements that have been included in statutes and regulations and the statutes of limitations that may apply to potential legal actions in which the records might be relevant.

2.2 Does the policy include a comprehensive records retention schedule that lists each of the categories of records generated or received by the company and the applicable retention periods for each of the records categories? The schedule should include descriptors such as record series title, description, retention periods, and special notes on handling of certain records.

2.3 Does the policy establish procedures for record storage and disposition and establish a central registry and depository for retained files? The policy must provide for prompt purging and destruction, on a regular basis, of records that have completed their respect retention periods.

2.4 Does the policy establish procedures for required retention of records in the event that a legal duty to retain and not destroy those records arises due to receipt of a threat of a lawsuit, governmental investigation or audit (not in the ordinary course of the company's scheduled financial reporting) involving the company? Suspension of records destruction in these instances is referred to as a "litigation hold" and should be handled carefully, particularly in the case of electronic records such as e-mail messages.

2.5 Does the policy discuss compliance with applicable laws and regulations pertaining the storage and preservation of records including conversion of paper records to

electronic records? The administrator should consult with legal counsel before proceeding in order to make sure that all applicable legal requirements have been satisfied. Examples include rules promulgated by the Internal Revenue Service regarding the use of automatic data processing systems to store transactional records that may be subject to audit in the future.

3. Administration and Audit

3.1 Does the policy assign responsibility for creating, administering, auditing and amending the policy? This type of policy is typically overseen by a "records administrator" appointed by senior management who is responsible, with his or her staff, for establishing a framework for categorizing information, setting up systems to track where records are located at any point in time, auditing compliance with the policy, making sure that records are promptly purged when they have reached the end of their designated retention period, amending the plan to take into account changes in technology and the company's business activities, and training employees on how to create and store records.

3.2 Does the policy establishing audit procedures and provide for the conduct of regular reviews to ensure that changes in regulatory requirements and records technology are reflected in the policy (*e.g.*, changes to required retention periods under applicable laws and regulations)?

3.3 Does the policy impose a duty on the records administrator to establish and coordinate implementation of procedures for conducting a company-wide review of all records that have not yet been moved to a central storage capability to determine whether such records can and should be moved to the storage capability or purged and destroyed as no longer being necessary under the applicable records retention schedule? The records administrator should develop checklists that can be consulted when auditing the records created or received by particular employee including reminders about the types of records they might have and where they might be stored.

3.4 Does the policy establish procedures for amending and replacing the policy, as well as granting waivers to the application of the policy, and clarifying whether records in existence prior the adoption of the policy are subject to its requirements? For example, if the company becomes involved in new business activities it will likely become subject to a host of different statutes and regulations that have their own unique records retention requirements and it will thus be necessary to make amendment to the existing policies and procedures.