InfoPAK<sup>SM</sup>

Effective Records Management

Sponsored by:

Jordan Lawrence<sup>™</sup>
Effective Records Management

September 2012

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

Records management is a critical issue for every organization, regardless of size or industry, to address. Effective records management insures compliance with regulatory obligations, results in lower costs, reduced risk and provides greater efficiency. Today, in-house counsel with responsibility for records management face an entirely new set of considerations and challenges than they did just a few years ago. This InfoPAK has been developed for in-house counsel to serve as their definitive guide to developing, implementing and consistently executing a practical and effective records management program.

The information in this InfoPAK should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Jordan Lawrence Group, L.C., or ACC or any of its lawyers, unless so stated. This InfoPAK is not intended as a definitive statement on the subject, but rather to serve as a resource providing practical information for the reader.

Jordan Lawrence Group, L.C., a long-term ACC Alliance Partner, developed the information contained in this InfoPAK under the direction and guidance of the Association of Corporate Counsel.
## Contents

I. Introduction ...................................................................................................................................... 6  
   A. Records vs. Information ..................................................................................................................... 7  
   B. Not all Policies are Treated Equal ........................................................................................................ 7  
   C. People, Processes, and Technology ...................................................................................................... 7  

II. Taking the First Steps ....................................................................................................................... 8  
   A. Records Inventory ("RI") ..................................................................................................................... 8  

III. Developing an Actionable Retention Schedule .............................................................................. 9  
   A. Retention Schedule Development Considerations: .................................................................................. 9  

IV. A Records Policy That Works ....................................................................................................... 10  
   A. Policy Objective / Purpose .................................................................................................................... 10  
   B. Policy Scope ......................................................................................................................................... 10  
   C. Roles and Responsibilities ..................................................................................................................... 11  
   D. Records Disposal / Deletion / Purge / Destruction ............................................................................ 11  
   E. Legal Holds ........................................................................................................................................... 11  
   F. Training .................................................................................................................................................. 11  
   G. Disciplinary Action ............................................................................................................................... 12  
   H. Audit ........................................................................................................................................................ 12  

V. Management of Email .................................................................................................................... 12  
   A. Key Considerations ............................................................................................................................... 12  
      1. Email Policy Scope ............................................................................................................................... 12  
      2. Retention Requirements for Email Retention .................................................................................... 13  
      3. The Business Reference Value of Email ............................................................................................. 13  
      4. Auto-Deletion Considerations ............................................................................................................ 13  

VI. Bringing Order to Unstructured Content with Microsoft SharePoint ........................................... 16  
   A. File Plan Brings Order to Unstructured Content .................................................................................. 19  
   B. The Perfect File Plan ........................................................................................................................... 19  
   C. File Plan Integration ............................................................................................................................. 20  

VII. Volume Correction ......................................................................................................................... 20
A. Key Considerations ................................................................. 21
B. Volume Correction Strategies ...................................................... 21
   1. Understand Current Media Holdings ........................................ 21
   2. Determine Business and Regulatory Value of Information in Specific Media .......... 22
   3. Apply Appropriate Retention Standards to Valid Business Records .................. 22
   4. Tag Records Required for Permanent Retention and Legal Hold ...................... 22
   5. Create Safe Standards that can be Implemented for All Non-Records ............... 22
   6. Communicate the Volume Correction Plan VCP ........................................... 22
   7. Implement Volume Correction Plan VCP ................................................ 22
   8. Schedule Routine, Non-Selective Disposal Events ........................................ 22
   9. Track Results ........................................................................... 23
C. Volume Correction Strategies for Email ....................................... 23
D. Volume Correction strategies for File Shares and Unstructured Content ............... 23
E. Volume Correction Strategies for Paper Records .......................................... 23
F. Capture Critical Information about Boxes: ........................................... 23

VIII. Personally Identifiable and Sensitive Information ............................. 24
A. Personally Identifiable and Sensitive Information ................................... 24
B. Key Considerations ......................................................................... 26
   1. Complete a Personal Data Inventory ............................................. 26
   2. Ensure Detailed Tagging for All Records and Information ....................... 26
   3. Complete Threat Assessments .................................................... 26
   4. Establish and Automate All Governance Rules and Policy Directives ............. 27
   5. Maintain Proper Reporting and Analytics for Continual Program Improvement .......... 27
C. Privacy Program Considerations ..................................................... 27
   1. Assess First, Then Remediate ..................................................... 27
   2. Records on All Media ................................................................ 28
   3. Privacy Programs on a Budget ................................................... 28
   4. Country-Specific Programs ........................................................ 28
   5. Continued Enforcement ................................................................ 28

IX. E-discovery ................................................................................. 28
A. Two Ways to Reduce E-Discovery Costs and Risks ................................................................. 29
   1. Develop a Discovery Data Map ......................................................................................... 29
   2. Eliminate Obsolete Records and Information ................................................................. 29
B. Managing Litigation Holds ................................................................................................. 29
   1. Primary Hold Management Obligations ......................................................................... 30

X. Conclusion ......................................................................................................................... 32
XI. Appendix ........................................................................................................................ 33
XII About Jordan Lawrence .................................................................................................... 41
XIII. Endnotes ....................................................................................................................... 43
### I. Introduction

Records management is a good business practice, the cornerstone of effective governance, and a requirement for companies operating in the United States and throughout most of the world. It is critical for senior management to understand five facts about records management.

First, it is the law. There are a multitude of state and federal regulations that require companies to retain a host of records for minimum time periods. The specific requirements, as well as consequences for not complying, vary widely by regulating authority. A common practice in many governmental inquiries is to leverage record retention regulations and test the effectiveness of company’s records management programs by making broad demands for records. Depending on the action or inquiry, failing to produce records that are required to be maintained, or even a delay in producing records, can result in severe consequences. Unfortunately, government agencies do not operate with the same consideration of “reasonability” that exists in commercial litigation. Companies must have confidence that they are meeting the minimum requirements for records retention, and that they can produce requested records quickly.

Second, many corporate records contain personally identifiable and sensitive information. Retaining these records any longer than is necessary to meet regulatory or business requirements creates unacceptable risk. Legacy records tend to not have the same degree of care and security as active records and, consequently, a high percentage of data breaches in the US involve inactive and legacy records that the business was not required to retain and that should have been deleted or destroyed. This fact has not gone unnoticed by legislators, and there is a new trend in privacy legislation, both domestically and abroad, to create maximum retention timeframes for records that contain personally identifiable information. Outside of the US, penalties can run as high as $1.5 million for keeping records containing personally identifiable information longer than permissible.¹

Third, as much as 60% of current litigation costs go to discovery and review of records.² A recent study by the Searle Center on Law, Regulation, and Economic Growth at Northwestern University found that only 1 in 1,000 pages produced in discovery is ever actually used as evidence to resolve the merits of the case. An effective records management program allows companies to defensibly delete and/or destroy a majority of records prior to a litigation event. Thus, an effective record retention program can dramatically lower the cost of litigation.

Fourth, significant costs are attached cost attaches to the storage of records that are not required by law or for a business reason. Electronic storage and physical offsite inventory costs increase as companies continue to over-retain records. A records management program enables a company to defensibly eliminate records, resulting in a substantial and tangible storage savings.

Fifth, the consequences for a company that experiences of a loss of vital records can be devastating. An effective records management program helps ensure that vital records needed to re-establish and continue operations are identified, and is a critical component of every Business Continuity Plan.

Records management adds value to any business by dramatically improving efficiency, reducing risks, and delivering costs savings directly to the bottom line.
The benefits of effective records management include:

- Improved accuracy and accessibility of information;
- Compliance with regulatory obligations;
- Significantly lower storage costs;
- Reduced discovery risks and costs;
- Better leverage of technology; and
- Greater protection of personally identifiable and sensitive information.

Before getting into specific details of effective records management, it is important to cover a few challenges every company faces.

A. Records vs. Information

Employees create massive amounts of information every day, but much of that information is not truly a business record. If the business has not distinguished records from general information, then they tend to keep everything permanently or for a very long time. This problem of over-retention includes virtually all content a business creates, including spreadsheets, presentations, documents, system reports, voice, video, and the like.

B. Not all Policies are Treated Equal

While most organizations have some form of a records management policy, seldom does the records management policy carry the same degree of concern and diligence as other corporate policies. Corporate records policies are commonly outdated, inadequate, ignored, and knowingly circumvented. Compliance is almost always left to the discretion of the individual employee, and compliance is seldom audited.

C. People, Processes, and Technology

To the extent possible, the records retention policy should be tied into applications and processes, thus enabling automation. The reality, however, is that “people” maintain and control a good deal of an organization’s records and information. A successful records management policy and strategy must contemplate people as well as technology. The policy should define time periods in which specific records should be retained, when that time period begins to run, and when they should be destroyed.

This InfoPAK has been carefully developed for in-house counsel to serve as their definitive guide to developing, implementing, and consistently executing a practical and effective records management program.
II. Taking the First Steps

The first steps taken in any records management initiative are creating an accurate records inventory and performing a risk assessment. The results of a risk assessment and records inventory form the foundation of an effective records management program. Most organizations have some sort of a records retention policy and schedule, but rarely do they reflect actual practices throughout the company.

A records inventory ties retention rules to where the records actually live, and it operationalizes the retention schedule. The risk assessment should evaluate the risks created by the business’s current records and information management practices — be they financial, legal, or both. By having a clear understanding of risks and opportunities, it is much easier to optimize policies, procedures, and technology to ensure the greatest chance for success.

A. Records Inventory (“RI”)

In order to meet these objectives, a company must look inside the business practices and talk to its employees. After all, they are really the only ones who know what records and information they have and use, where they retain them, the media types, the storage locations where they reside, and how long they retain and reference records and information. The records inventory is the “roadmap” for executing the policy. (Refer to Appendix A to see an example of a Perfect Records Inventory.)

The Records Inventory should:

- Be a detailed listing of the records types that employees work with day in and day out, and is derived by profiling business representatives from each business area.;
- Identify current practices,, including the media and applications where the record types exist, and which specific version is the official version or a convenience copy.;
- Document how long the business area requires access to the specific record type, and how long the record type is being retained.;
- Identify the sensitive elements found within each record type, which will ensure that sensitive information is appropriately identified, managed, and safeguarded; and
- Identify where employees get records, where the save them, and who and how they share records.

In addition to profiling employees, it is critical to profile individuals who have specific functional expertise about the information technology (“IT”) infrastructure. These individuals would include subject matter experts within fields such as email administration, email backup, file server administration, file server backup, desktop administration, backup processes, and physical records storage.

By gathering this information from all the different areas and subject matter experts, a company will have a clear understanding of its current records practices, which in turn will help it make
better decisions about information management going forward.

III. Developing an Actionable Retention Schedule

Retention schedules are often confusing and complex; they force employees to make judgment calls about how to classify records, how long to retain them, and where to retain them. When employees need to exercise discretion, the results will assuredly be inconsistent. The retention schedule should be clear and concise, avoid ambiguous language, and reflect the actual records that the organization maintains. (Refer to Appendix B to see an example of a Perfect Retention Schedule.)

The employee profiling process leads to a retention schedule specifically designed for the company’s functional or departmental structure, division or subsidiary structure, and technology infrastructure. The result is greater compliance, increased records retrieval and discovery efficiency, and greater accountability and ownership by employees.

Statutory requirements are often ambiguous and rarely provide definitions of record types. The retention schedule needs to provide clear definitions, descriptions, and a definitive trigger. As few as 60% of actual records have regulatory requirements, and the rest are retained to support business needs.3

A. Retention Schedule Development Considerations:

- **Formats of the Retention Schedule**
  - **Retention Schedule by Record Type** is a listing of record types in alphabetical order, and is not associated to specific areas or departments. Every employee accesses the same list to locate records. This is an approach that best fits smaller organizations or organizations with few record types.

  - **Retention Schedule by Function** associates record types to their function, area, or business. For example, all human resources (“HR”) records are presented on an HR Retention Schedule. Every employee may be provided access to the various functional schedules, or instead granted access only according to their specific areas of responsibility.

- **Taxonomy**: Record type naming standards are set across the company to define the language of the retention schedule. Keep naming standards simple and broad in order to ensure greater employee understanding and adoption. Descriptions provide the details of what type of information record types typically contain; those descriptions also help simplify search efforts when records are needed.

- **Scheduling Logic**: It is important to document the various decisions that were made when determining retention periods or “Scheduling Logic”. It provides the “logic” of how federal, state, industry practices, and/or business-defined requirements were applied. However the company chooses to develop finalize its scheduling logic, the process should focus on including internal review, best practices, and legal review.
Tagging: Various requirements, beyond retention, determine the appropriate management of certain record types. Special tagging, such as sensitive information, data classification, and various regulatory requirements, help direct employees to take special actions.

Triggers: Where applicable, triggers should be applied to denote the date on which to “start the clock” for the duration of time that a document should be kept prior to destruction.

The Retention Schedule is the basis for the legal and defensible disposal of records. Its accuracy is important to ensure information is maintained no shorter or longer than the appropriate time period. The company should undertake an annual review of the schedule by a team of functional representatives. This is a good opportunity to make intentional updates, as the method of managing certain documents might have been changed from the previous year. These updates will be beneficial for ongoing policy compliance and employee adoption.

IV. A Records Policy That Works

Most companies have, to some degree, a Corporate Records Policy; nevertheless, the policy often is incomplete, difficult to understand, in conflict with other existing policies, or never enforced. The following key components should be considered when enforcing the Corporate Records Policy.

A. Policy Objective / Purpose

Companies need to understand their risks and opportunities in order to clearly define the policy objective. Hence, the first step should be to complete a records inventory and risk assessment. Determine what the reader (employee) should “take away” after reading the policy.

It is important to tailor the policy objective/purpose to the individual company, by considering functions, departments, and infrastructure, rather than simply adapting a policy that was created with a different organization in mind.

B. Policy Scope

It pays to outline exactly who and what is subject to the policy.

Consider the following aspects:

- Does the policy apply to all record types, regardless of media?
- Do employees understand what information is the company’s, versus what is theirs?
- Do employees understand that records they store at their residence or in the cloud may actually belong to the company?
- Have official records and record types been clearly defined?
This information is important for employees to have a better understanding of what they are expected to do in order to be compliant with the Corporate Records Policy, Email Policy, Electronic Use, and other policies.

C. Roles and Responsibilities

It is essential for the legal function to work with Information Technology and Audit when developing the policy, as well as with certain business operations, — especially when the company is in a highly regulated industry (e.g., financial institutions, aerospace and defense, or the food industry). Technology processes and policies need to be aligned to the Corporate Records Policy; furthermore, the Technology Department needs to be aware of the expectations of the legal group. From an audit perspective, they need to be aware of the corporate objectives so they can plan accordingly and ensure ongoing departmental compliance throughout the organization.

Additionally, identifying and defining employee responsibilities will make these staff members an important part of the Corporate Records Program, creating accountability and ownership.

D. Records Disposal / Deletion / Purge / Destruction

Without destruction, records management is simply records retention. Most records are only an asset of the organization for a relatively brief time. It is in the best interest of the company to purge records once they have fulfilled their legitimate retention requirement. Disposition and destruction of records is a very important component, yet many policies fail to address the actions that employees (e.g., Records Managers, IT personnel, offsite storage vendors) are to take when retention periods have been reached. The policy must institute and communicate consistent destruction practices to reduce risks and costs.

E. Legal Holds

In the event of pending or imminent litigation, audit, or government investigation, companies have a legal responsibility to enact and enforce hold orders; best practice is to have the orders in writing. Unfortunately, few companies have adopted an automated, secure, and repeatable process for doing so.

Companies need to establish a centralized and verifiable legal hold process, and document it as part of the Corporate Records Policy.

F. Training

Records management issues are typically people issues, rather than technology issues. Research shows that more than 40% of employees on average are not aware of their company’s Corporate Records Policy, and 54% of employees don’t believe the Corporate Records Policy applies to email or electronic records.

A successful records program requires regular communication and training. The best policy in the world doesn’t mean much unless employees are aware of it, trained to understand how to comply
with it, and knowledgeable of where to go when they have questions. Companies cannot claim to have implemented a sound records program unless they provide regular and comprehensive training in this area to their employees.

G. Disciplinary Action

Seldom will people do what they should do without an external motivation or consequence. Disciplinary action, and the fear that accompanies it, provide the necessity for employees to comply with the Corporate Records Policy. It is important to clearly state the repercussions that employees can expect if they choose not to follow the policy. Don’t handle this lightly; the policy is in place for a reason.

H. Audit

Last but not least, it is necessary to put some punch behind the Corporate Records Policy by instituting a regular audit. This is likely the time when a company will find out if everyone is adhering to the policy as required. Whether related to the Sarbanes-Oxley Act or other internal audit purposes, a company must work with an audit group to ensure appropriate audit mechanisms are in place, and that the auditors are highly trained in understanding the policy, retention schedule, legal hold, and disposition processes.

The creation and implementation of a records retention program is one that should not be taken lightly. To post a policy in a remote location on your intranet is not responsible information management. Compliance is an ongoing effort to educate employees, distribute policies, and update the retention schedule. Routinely acting on destruction and other policy directives mitigates risks, as well as reduces the costs associated with volume growth.

V. Management of Email

The majority of email consists of non-records that provide no business value; instead, they exist as white noise on organizations’ servers, eating up space and presenting a significant discovery risk. Over-retention of email increases electronic storage needs and collection efforts during e-discovery, producing unnecessary costs for companies. The development of a detailed email policy, followed by the disposal of applicable email records, is the key to getting a handle on the vast amounts of email corporations have today.

A. Key Considerations

I. Email Policy Scope

Implementing any type of email policy will impact more than just the end users. Current practices across all email server locations must be evaluated and updated to ensure consistency across the organization.
2. Retention Requirements for Email Retention

The majority of companies have no overarching regulatory requirements to retain email. The content of certain emails may be considered a “business record.” Some industries, such as broker/dealers, have specific regulations defining how long email must be retained. These regulations are typically isolated and very specific. As a result of the records inventory, counsel should have a view of these types of situations.

Decisions can be made regarding the effectiveness of using email as the primary record. Alternatively, processes can be changed and/or relevant email and attachments should be migrated outside of the email environment. Review and apply any applicable regulatory requirements that would govern the retention of email across the company or within specific areas of the company.

3. The Business Reference Value of Email

A common misconception is that email runs the company and is needed for long periods of time. Take the time to ask employees the necessary questions to determine the reference value of email; the actual reference value of email is relatively short. This can be accomplished through your records inventory. Consider the true business reference value of email across the company, and within business functions, to determine if valid business reasons exist that would influence the retention of email.

It is best to weigh the cost of retaining email to satisfy the anecdotal story “Remember that one time that we had to find that one email...” against the costs and risks of retaining emails that could be a liability to your organization.

4. Auto-Deletion Considerations

Auto-deletion timeframes routinely eliminate non-essential email, and alleviate the employees’ burden of manually deleting obsolete email. When no specific requirements have been established to retain email, the auto-deletion timeframes should balance business utility and corporate culture against the cost and risk of retaining email. Increasingly, companies find that retaining email for a shorter period of time lowers operational costs and reduces risk. The considerations outlined in this section can help define the right auto-deletion approach.

a. Segmenting Auto-deletion Rules

One approach for organizations to manage email is to set auto-deletion rules based on specific roles or levels of employees. It may be prudent to have a longer auto-deletion period for senior executives, and a shorter auto-deletion period for employees at an administrative level.

Here are some examples of email segmentation to consider:

- Example 1 — Set rules at employee grade level
  - Senior management and vice president (“VP”) levels – 3-year auto-delete
• Executive and director levels – 5-year auto-delete

■ Example 2 – Set rules based on job functions
• Broker-dealers – 3-year auto delete
• Customer-service representatives – 18-month auto-delete
• Engineers/scientists – 7-year auto-delete
• Field sales offices/plants – 18-month auto-delete
• Legal departments – 5-year auto-delete

b. Email Retention Folder Strategies

Another example of email segmentation is to set short-term auto-deletion standards across the organization, then establish special long-term retention folders to support email with longer-term business reference value or special business needs.

*Example of Stratified Email Retention 7:*
c. Maintaining an Email Journal

Email systems allow an on/off decision to maintain a journal of all emails sent and received from all or select email accounts. The majority of companies do not journal for all email users. Journaling email has tremendous impact on the cost to store and manage email, and directly impacts the search and review costs during litigation and discovery. It is critical for legal and IT to be on the same page when deciding if business or legal utility exists in journaling email for the company.

If there is a value in journaling email, then consider narrowing the scope to selected individuals, departments, or job levels to control the growth of email within the email system or archive.

d. Email Archiving Practices

Email archiving solutions address storage limitations and backup management challenges by offloading the email servers onto scalable and searchable archives.

Many companies believe that business records should not be managed in the active email environment, and should be moved to locations where similar business records are retained. Common locations include an email archive or document management systems such as SharePoint.

The ease of retaining and searching email can swing both ways during litigation; a consideration that has led many companies to conclude that archiving is not the right solution to control and manage email volume and growth. If the company already has an email archive or feels that the email archive is right for its needs, then ensure retention rules are also applied to the archive.

e. Backups vs. Archive

Backups contain a “snapshot” of information from a single instance in time. Because they are simply copies of the active server, backups look exactly like the active server at the time the backup was created. Backups are made at regular, predetermined intervals, and are often coded by a single date/time when the backup was created.

Email backups should be for disaster-recovery purposes only. Backup schedules and rotations should be adjusted to meet disaster-recovery needs, and must be aligned with the auto-deletion time period that has been established. This ensures that no lapses are created in the overall intentions of the policy.

Having an auto-delete policy, yet maintaining email backups indefinitely, is a contradiction. It does not eliminate any risk for the organization, as backups are discoverable if litigation occurs. Not aligning email policies with backup practices is one of the most common mistakes made regarding email.
f. **Prohibit Moving Email Outside of a Structured Environment**

To further manage email and associated storage and discovery costs, many companies prohibit employees from storing and saving email outside of centrally controlled environments. Prohibited locations typically include personal archives (PSTs or NSFs), local hard drives, personal cloud storage, and forwarding email to personal accounts, as well as removable devices such as compact discs (“CDs”), Universal Serial Bus (“USB”) flash drives, and digital versatile discs (“DVDs”). Many companies have IT turn off the ability for employees to create PSTs and NSFs, and specifically prohibit personal email archives.

g. **Email of Departed Employees**

Depending on email auto-deletion practices, the Email Policy should set clear standards that address the email content of departed employees.

h. **Prohibit Sending Sensitive Information in Email**

Many companies prohibit employees from transmitting sensitive information through standard, non-secure email in an effort to ensure the confidentiality and security of personally identifiable, corporate proprietary, and restricted information. Consider alternative methods that comply with the company’s security and data classification policies for sharing sensitive information within and outside the company.

i. **Litigation Holds**

The policy should also define the process for reviewing employees’ email to determine if it is subject to a litigation hold. Legal and IT should establish a formal process to ensure email and other electronic information can be locked down and protected from deletion when there is pending or imminent litigation.

VI. **Bringing Order to Unstructured Content with Microsoft SharePoint**

Unstructured electronically stored information (“ESI”) is everywhere (e.g., network shared drives, hard drives, laptops, CDs/DVDs, flash drives, and even uncontrolled content management systems). ESI volumes are growing more than 20% annually, and are rapidly becoming a primary concern to legal and IT professionals.8

The majority of ESI created and retained by business users is considered “unstructured” content. There is a high reliance on employee discretion in what the information is called, where it is stored, and how long it is retained. Only a small percentage represents valid business records, but all are discoverable and can cause great difficulty in production efforts.

Unfortunately, many organizations haven’t even thought about applying retention to unstructured content, because it’s been difficult to separate real records from all of the general information. Employees have almost complete control over the creation, naming, storage, and retention of
unstructured content. As a result, companies end up keeping electronically stored content on shared drives and user drives permanently or for excessively long periods of time.

Content Management (“CRM)” and Electronic Document Management (“EDM)” systems can be a viable solution to manage ESI, but only if appropriate retention rules are concurrently implemented.

This section focuses on Microsoft SharePoint for a number of reasons:

- Eighty percent of companies already use or have a SharePoint license, keeping implementation costs low or non-existent.  
- SharePoint integrates seamlessly with the Microsoft Office suite used by most companies, making user adoption easier.  
- The “In Place Records Management” feature in SharePoint makes it easy to manage records and non-records, with varying retention rules for each.

Another advantage of using SharePoint for managing electronic content is that Microsoft supports a robust ecosystem of partners and vendors that offer products and services exclusively to support SharePoint. Products range from defining file plans to seamlessly capturing, storing, and classifying content from scans, emails, and electronic documents in all forms into SharePoint, with little or no employee interaction. Similar to the App Store from Apple, there is a Microsoft Partner-supported solution to accomplish almost anything in this realm via SharePoint.

A way to manage this segmentation is to create repositories for daily work in progress files that are separate from records. These can be segmented by user, department, or project. The retention of these temporary repositories is usually short, and in specific relation to how long the information retains business reference value (for example, until the end of the project).

In order to retain information beyond this short retention period, users must either move documents from the work in progress location to a longer-term storage location or declare them as records. The retention periods for the long-term locations or records are typically based on legal or regulatory drivers (e.g., the retention schedule). The key is to make sure that all information has a disposition date tied to it. Establishing a process to eliminate general information quickly, and preserve records according to a legally defensible retention schedule, is an appropriate way to curb the electronic information overload.

As working documents become records, employees move them to the appropriate record libraries on the left side of the following image that have appropriate legal, regulatory, or business-driven retention policies associated to them. Employees don’t have to worry about retention, as it’s automatically applied to documents based on the libraries in which they’re located.
Example Microsoft SharePoint setup:
A. File Plan Brings Order to Unstructured Content

Completing a records inventory as described earlier provides the foundation needed to implement retention rules into Microsoft SharePoint. As promising as SharePoint is, putting content into it without solid and defensible retention rules just shifts the problem of ever-growing and unmanageable electronic information from file servers and other repositories. Developing a File Plan with retention rules is the fundamental, critical first step in making SharePoint a viable way to control content and to applying retention standards that protect your company’s legal and financial interests.

Like the records inventory, your company’s File Plan needs to reflect the business practices of its employees. Otherwise, companies struggle with program adoption, and SharePoint implementation can stall or even fail. Developing an effective file plan requires leveraging input from employees collected during the Records Inventory. Their insights provide the details needed for developing a File Plan that works.

B. The Perfect File Plan

A good File Plan contains a complete list of content types grouped by area or department. Each content type should be linked to a specific, legally defensible retention period. Developing a file plan in the format prescribed by Microsoft simplifies updating SharePoint with the company’s content types. The following example illustrates a well-structured file plan with necessary elements. This baseline information helps to determine the success (or failure) of adopting SharePoint.

<table>
<thead>
<tr>
<th>Content Type</th>
<th>Description</th>
<th>Category</th>
<th>Retention / Authority</th>
<th>Trigger</th>
<th>Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affirmative Action</td>
<td>Includes job descriptions and workforce analysis.</td>
<td>Benefits</td>
<td>3 years 29 CFR 1620.32</td>
<td>Closed</td>
<td>Destroy</td>
</tr>
<tr>
<td>Benefit Folders</td>
<td>Official documentation for employee enrollment in medical, insurance and 401K plans. Includes benefit cards, designation records, enrollment benefit notices, statements of health benefits, contributions, cobra records, etc.</td>
<td>Benefits</td>
<td>9 years 29 USC 1027</td>
<td>Closed</td>
<td>Archive</td>
</tr>
<tr>
<td>Benefit / Pension Plan</td>
<td>Official documentation for employees’ pension enrollment.</td>
<td>Permanent Corporate Standard</td>
<td>N/A</td>
<td>N/A</td>
<td>Archive</td>
</tr>
<tr>
<td>Disability Records</td>
<td>Items short- and long-term disability.</td>
<td>Benefits</td>
<td>12 years 29 USC 1027</td>
<td>Date of Claim</td>
<td>Archive</td>
</tr>
<tr>
<td>Drug Screening Records</td>
<td>Includes testing results and reporting.</td>
<td>Recruitment</td>
<td>3 years 29 CFR 1623:3</td>
<td>Completed</td>
<td>Destroy</td>
</tr>
<tr>
<td>EE0 Compliance</td>
<td>EEO-1, EEO-2, and annual affirmative action reports.</td>
<td>Recruitment</td>
<td>10 years Legal/Consideration</td>
<td>After Filed</td>
<td>Archive</td>
</tr>
<tr>
<td>Medical Files</td>
<td>Includes medical records, doctor notes, authorization for treatment.</td>
<td>Benefits</td>
<td>10 years 29 CFR 1904</td>
<td>Terminated</td>
<td>Archive</td>
</tr>
<tr>
<td>Payroll Records</td>
<td>Payroll changes, check registers, deductions, earning reports, attendance records, time sheets, incentive awards, reconciliation reports, etc.</td>
<td>Payroll</td>
<td>8 years State/Payroll</td>
<td>After Paid</td>
<td>Archive</td>
</tr>
<tr>
<td>Personnel Files</td>
<td>Personnel files including employee reviews, appraisals, disciplinary actions, status changes, compensation agreements, employee agreements, non-disclosure agreements, non-compete agreements, exit interviews, etc</td>
<td>Employment</td>
<td>8 years State/Payroll</td>
<td>Terminated</td>
<td>Archive</td>
</tr>
</tbody>
</table>
Many companies develop File Plans that simply list department names and record types, or they try to use their existing and outdated retention schedules. Without a properly formatted file plan with content types and retention standards that sensibly map to the day-to-day operations of the employees, their SharePoint implementations fall short.

C. File Plan Integration

Once a well-formatted File Plan is established, it should become the roadmap for SharePoint implementation. IT can use the File Plan to determine:

- Sites and sub-sites to create based on areas of the file plan;
- Content types to create;
- Retention policies to establish for each content types; and
- Document libraries to create.

When employees create records in SharePoint, they inherit the retention rules from the content types created from the Records Inventory.

VII. Volume Correction

Companies that have not effectively managed records retention in the past generally find they have crushing volumes of legacy and redundant records and information. This creates a number of issues, including excessive storage costs, inefficiencies locating needed information, increased exposure to data breach, and increased risks and costs during discovery. This section is designed to enable companies to make strategic decisions that eliminate legacy and redundant records and information without taking undue risk. The considerations within this document should be undertaken only upon the advice of the company’s legal counsel, as well as other senior advisors and subject matter experts.
A. Key Considerations

For many companies, significant advantages may be realized from reducing volumes of information. Aside from cost reduction, many companies see significant improvements in business efficiencies.

Consider the following points:

- It is wasteful to retain unnecessary records. The cost of storage is high, and this cost increases as more storage capacity is required. If the company implements and enforces a Records Retention Policy, the volumes of retained legacy data could drop as much as 30% to 60%.vi
- Volumes are only going to increase. Without action now, the amount of information a company will have in ten years will be unmanageable. The effective solution is not adding more capacity and establishing faster searching.
- Consider the value of the information.. Most business representatives profiled indicate that the reference value of information in general drops significantly over time.10 Understanding the reference value provides a baseline for setting retention for general information.
- Email that contains personally identifiable and sensitive data constitutes an immense risk to companies. To meet legal obligations as well as to protect the company, customers, and employees, it is critical to appropriately eliminate legacy data as soon as it meets retention or business needs.
- Establish better decision making. The data handling and storage decisions that are made at current volumes are very different than those that would be made at a fraction of the volume. Cost savings and risk reductions will be dramatic.
- Determine any current legal holds that affect the legacy records.

B. Volume Correction Strategies

Volume correction strategies are pretty straightforward, and can align with different media used throughout the company. Once an appropriate records inventory has been developed, a company can filter on specific media and come up with defensible standards for moving forward. Follow these steps to ensure consistency.

I. Understand Current Media Holdings

Understanding the scope of your information holdings is extremely important in terms of consistency. This includes information contained on servers and in storage locations onsite as well as offsite.
2. Determine Business and Regulatory Value of Information in Specific Media

By analyzing the records inventory and determining the business reference value of information, one can determine the sort of information that needs to be retained for longer periods of time. This process may require record sampling or other defensible methodologies.

3. Apply Appropriate Retention Standards to Valid Business Records

Apply the retention schedule according to the retention requirements for the company’s information.

4. Tag Records Required for Permanent Retention and Legal Hold

Consult with the legal function to compile a list of all active holds. Use key words, departments, regions, lines of business, and date ranges to refine and identify records correlating to active holds.

Perform keyword searches for permanent records. Tagging permanent records helps protect, from disposal.

5. Create Safe Standards that can be Implemented for All Non-Records

Safe standards can be applied across media or departmentally. The idea of safe standards is to simply apply a retention period to all information that has not been classified as a specific business record.

6. Communicate the Volume Correction Plan

Make sure everyone in the organization understands the program’s objectives and goals. With such communication, all stakeholders can work together to generate success.

7. Implement Volume Correction Plan

Work with the appropriate custodians to dispose of obsolete information. This could involve system administrators, storage warehouses, or departmental employees who are looking to clean up their work spaces.

8. Schedule Routine, Non-Selective Disposal Events

Direct system administrators, employees, and storage providers to consistently dispose of business records when they have met their retention requirements.

Employees should not obstruct the routine disposal process. If a need to suspend normal destruction occurs, then employees should contact the legal department with a valid business or legal reason. Legal decision-makers should have the final approval to place a litigation hold.
9. **Track Results**

A company that implements these strategies should consider tracking the “before” and “after” environment not only to quantify success, but also to provide an audit trail.

**C. Volume Correction Strategies for Email**

Email is generally the “problem child”; it proliferates throughout the company, is extremely redundant, and consumes tremendous resources to manage and store. Email communication has become so common that it represents the single greatest risk to the company in the context of litigation. Consider the email strategies documented in previous sections, and don’t forget to look into the archive and backup processes.

**D. Volume Correction strategies for File Shares and Unstructured Content**

The majority of electronic information created and retained by business users on shared drives is considered unstructured content. Unfortunately, in most organizations, unstructured content is retained indefinitely due to lack of rules, no routine deletion, and no employee responsibility. For most departments, only a small fraction of the electronic information saved on network drives constitutes actual business records that have a legal, regulatory, or valid business requirement to be retained. Once they have met their retention needs, these records become a liability.

Implementing safe standards at the departmental level will help ensure that these legacy records are not continually maintained, and reduce the liability to which the company may be exposed.

As mentioned with regard to email, make sure that backup and archive strategies align with the company’s safe standards and overall records program objectives. Many times these are forgotten processes, and end up costing the company in the long run.

**E. Volume Correction Strategies for Paper Records**

With so much current attention focused on email and electronic records, it is important that companies not overlook the significance of “old fashioned” hardcopy paper records, as well as the policies and practices that companies have in place to manage them.

 Appropriately, apply retention to legacy boxes, and make sure that the company introduces practices so that this “mess” doesn’t occur in the future.

**F. Capture Critical Information about Boxes:**

The following box information should be captured in a centralized company-controlled database for all boxes going to storage (whether at vendor or company-operated facilities):

- Valid department name/number and originator’s name;
In consideration of security, consistency, and accuracy, maintain a detailed box inventory in a centrally controlled database that is vendor- and facility-neutral. Those charged with physically handling boxes should not be privy to the contents. Additionally, in-house counsel must consider the issue of rights management regarding paper records. In other words, paper records and electronic records should be given the same considerations for rights management.

VIII. Personally Identifiable and Sensitive Information

The development of a legally defensible privacy program has become an obligation that cannot be ignored; the risks and penalties are too great. In addition, the company’s customers and employees, the public, and regulators have ever-increasing expectations regarding privacy.

Privacy obligations create some of the most serious legal and financial risks that companies face. As a practical matter, companies need to understand and address the basic obligations as quickly and cost-effectively as possible. Baseline information will provide the fundamental building blocks of a successful program.

A. Personally Identifiable and Sensitive Information

Personally identifiable information (“PII”) is classified as “information” that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.11

Sensitive information (“SI”) is classified as privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it.
Example of PII and SI:

<table>
<thead>
<tr>
<th>Personal Identification</th>
<th>Financial Information</th>
<th>Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veteran Status</td>
<td>Bank Account Number</td>
<td>Copyrights</td>
</tr>
<tr>
<td>Marriage Status</td>
<td>Bank Routing Number</td>
<td>Patents</td>
</tr>
<tr>
<td>Family Information</td>
<td>Credit Card Number</td>
<td>Trademarks</td>
</tr>
<tr>
<td>Name</td>
<td>Debit Card Number</td>
<td>Engineering/Design</td>
</tr>
<tr>
<td>Gender</td>
<td>Billing/Account Information</td>
<td>Documents</td>
</tr>
<tr>
<td>Email Address</td>
<td>Credit History</td>
<td>Product Specifications</td>
</tr>
<tr>
<td>Physical Address</td>
<td>Retirement Account Number</td>
<td>Lab Notebooks</td>
</tr>
<tr>
<td>Citizenship Status</td>
<td>Retirement Account Balances</td>
<td>Trade Secrets</td>
</tr>
<tr>
<td>Telephone</td>
<td>Insurance Information</td>
<td>Other IP</td>
</tr>
<tr>
<td>Birth date</td>
<td>Tax Information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employment Information</th>
<th>Patient Health Information</th>
<th>Sensitive Information (EU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employment Status</td>
<td>Patient Name</td>
<td>Ethnic Origin or Race</td>
</tr>
<tr>
<td>Wage Garnishment</td>
<td>Patient Address</td>
<td>Political Party of Affiliations</td>
</tr>
<tr>
<td>Information</td>
<td>Dates (admission, discharge, death)</td>
<td>Religion</td>
</tr>
<tr>
<td>Resume</td>
<td>Medical Record Number</td>
<td>Philosophical Beliefs</td>
</tr>
<tr>
<td>Job History</td>
<td>Health Plan Beneficiary Number</td>
<td>Health Status</td>
</tr>
<tr>
<td>Employee ID</td>
<td>Device Identifiers and Serial Numbers</td>
<td>Sexual Orientation</td>
</tr>
<tr>
<td>Medical Conditions</td>
<td>Biometric Identifiers</td>
<td>Criminal Records</td>
</tr>
<tr>
<td>Handicapped Status</td>
<td>Photo Images</td>
<td>Trade Union Membership</td>
</tr>
<tr>
<td>Professional Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compensation Information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Corporate Confidential</th>
<th>Government Issued IDs</th>
<th>Physical Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Financial</td>
<td>Social Security Number</td>
<td>Height</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Business Plans</td>
<td>Partial Social Security Number</td>
<td>Weight</td>
</tr>
<tr>
<td>Sales Plans</td>
<td>Social Insurance Number</td>
<td>Eye Color</td>
</tr>
<tr>
<td>Marketing Strategy</td>
<td>National ID Card Number</td>
<td>Voice Imprint</td>
</tr>
<tr>
<td>Merger/ Acquisition Plans</td>
<td>Driver's License Number</td>
<td>Retina Scan</td>
</tr>
<tr>
<td>Legal Actions</td>
<td>Passport Number</td>
<td>Fingerprint or Handprint</td>
</tr>
<tr>
<td>Contractual Info</td>
<td>Other Biometric Data</td>
<td>Other Biometric Data</td>
</tr>
</tbody>
</table>

## B. Key Considerations

Regardless of company size or industry, the following basic steps should be completed to meet primary privacy obligations and enable companies to move ahead in solving more-complex issues.

1. **Complete a Personal Data Inventory**

Companies should develop and maintain a comprehensive inventory of PII and SI. This is a foundation for meeting all legal and business obligations. (Refer to Appendix D to see an example of a Perfect Personal Data Inventory.)

2. **Ensure Detailed Tagging for All Records and Information**

More than 100 defining elements must be considered to complete a comprehensive Personal Data Inventory (“PDI”). Key tags that should be defined for records information include the following:

- Tag PII and SI that may exist within each business record.
- Regulatory tagging for non-retention requirements provides compliance and legal professionals with needed information for policies and necessary actions related to information subject to relevant legal requirements, such as the Health Insurance Portability and Accountability Act (“HIPAA”).
- Distribution patterns uncover which records are distributed within and outside of the organization. During data inventory collection, most companies find many instances of risky movement of PII and corporate SI. Armed with definitive insights and proper enforcement automation, companies can implement corrective policies, directives, and accountability audits.

3. **Complete Threat Assessments**

Companies must complete periodic Threat Assessments to identify and protect PII and SI.
4. Establish and Automate All Governance Rules and Policy Directives

A limited number of routine communications are needed for a legally defensible and risk-controlling privacy program.

For maximum compliance, all communications should be calendared for automatic distribution (proves consistency) to preset distribution lists (proves non-selectivity), and employ automation that demands compliance verification from each recipient (proves diligence).

5. Maintain Proper Reporting and Analytics for Continual Program Improvement

Sensitive Information Inventories and Threat Assessments should be maintained and kept completely updated.

Data maps are comprehensive and specific inventory listings that should be maintained to help the company identify and address the areas of greatest risk, and efficiently address applicable legal requirements.

Statistical Reports provide immediate overviews into every aspect of current practices, and lead to other reports for more detail along with actions that lead to opportunities for better compliance.

C. Privacy Program Considerations

With what seems like daily headlines of identity theft and losses of personal data, the pressure on privacy officers is at an all-time high. Organizations face new threats to personal data, and new legal requirements for privacy put pressure on companies to heighten security regarding this information.

Companies face a number of common hurdles when developing a successful privacy program.

1. Assess First, Then Remediate

A sound privacy program encompasses more than a written policy or a set of guidelines. All companies and organizations should conduct periodic risk assessments to determine if any gaps or vulnerabilities exist in their information security and data protection programs.

The assessments should collect details regarding sensitive information by location, media used, authoring application, record types, how data is used, how it is distributed, and if it is held by third parties. The information should be organized by type of personal data (e.g., sensitive data or health data).

Every company should maintain up-to-date information that provides visibility into its current practices. This updated inventory will reveal privacy vulnerabilities in the management of records, email, unstructured content, over-retention, and duplicate retention of information.
2. **Records on All Media**

Breach-notification laws apply to electronic information and records in physical form as well. Many stories exist of briefcases or boxes containing sensitive information in paper form that end up in the wrong hands and cause significant data breaches.

3. **Privacy Programs on a Budget**

Contrary to popular belief that privacy can only be addressed by adding expensive new technology, companies frequently find that existing technology can be implemented to address privacy needs. Encryption of notebook computers and portable devices prevents unauthorized use in the event that the devices are stolen or lost. Encryption of computers can also provide a “safe harbor” in the context of U.S. breach-notification laws which would otherwise require notification of customers if data on a lost device was not encrypted.

4. **Country-Specific Programs**

Breach-notification requirements and strict privacy laws put an additional burden on enterprises in the U.S. and Europe. The first step in privacy initiatives that extend beyond national boundaries is to develop a clear understanding of the privacy standards in all countries where the organization operates.

Privacy guidelines must be country-specific, because legal requirements differ and sometimes contradict each other. For example, in the U.S. employers are allowed broad discretion in monitoring employee email and internet use, whereas the European Union nations, for example, strictly limit employee monitoring.

5. **Continued Enforcement**

A successful privacy program is not about conducting the assessment once and writing a policy. It takes continued efforts to ensure proper measures are in place and aligned with the potential threats and risks. Only then can a company demonstrate that a privacy program has been routinely enforced.

**IX. E-discovery**

Most discovery challenges stem from unenforced records policies and over-retention. It is a waste of time and money to search through unnecessary records that could have been disposed of in the normal course of business under a sensible policy.

Faster search is seldom the answer to discovery problems. Companies that invest in enterprise search technologies often find that their review costs actually increase as more data is captured. If information is available, then it is discoverable. Even innocent records — in the hands of a skilled adversary — can be shown out of context and used effectively against a company. This can lead to unnecessary settlements and adverse judgments.
Companies and their legal adversaries alike recognize that poor enforcement of retention requirements means that potentially responsive information could be anywhere; finding it means sifting through massive volumes of information, at great cost and disruption to business. Many attorneys feel they have few alternatives other than a large-scale (and costly) production. Increasing numbers, others find themselves opting for expensive settlements, regardless of the merits of the case, as the better financial option.14

Proper records management policies and retention schedule compliance not only reduces the amount of official records companies store; it also creates best practices among their employees to reduce other information not subject to retention that may otherwise be discoverable.

A. Two Ways to Reduce E-Discovery Costs and Risks

1. Develop a Discovery Data Map

The risk companies face in e-discovery is not the “smoking gun” document; it’s not knowing what potentially responsive records and information exist and where to look. Developing a Discovery Data Map that identifies what records exist, where they are stored, and who owns them will increase the effectiveness and efficiency of the e-discovery process. (Refer to Appendix C to see an example of a Perfect Discovery Data Map.)

2. Eliminate Obsolete Records and Information

The way to really discovery costs and risks is thorough, judicious execution of the company’s records retention policy prior to any foreseeable litigation. In addition to looking for ways to search for and review documents more effectively and efficiently, companies should identify what records and information they have that can immediately be disposed. When that is done, most problems and costs related to e-discovery will no longer exist.

B. Managing Litigation Holds

An effective records management program must contemplate the suspension of routine, defensible destruction in the event of possible or actual litigation or investigation. To meet hold obligations, companies need a repeatable, consistent process to identify responsive parties or records; communicate the orders, and track, manage, edit, and release hold notifications.

A legal hold notification is a communication issued as a result of current or anticipated litigation, audit, government investigation, or other such matter that suspends the normal disposition or processing of records. The specific communication to business or IT organizations may also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice."

The idea of issuing litigation holds is not new, but in the case of Pension Committee vs. Banc of America, Judge Shira Scheindlin provided exceptional detail for hold management practices.15
I. Primary Hold Management Obligations

Proper hold management integrates quality records-management practices with a streamlined approach for issuing hold notifications. Corporate information should follow strict taxonomy standards, provide a roadmap of all record types and information across all media, and be governed by a consistently enforced Disposal Policy. Hold management works hand-in-hand with records management. With proper records management, these hold management obligations will help an organization achieve faultless and defensible hold notification processes.

a. Timely Issuance

A legal hold should be issued long before an actual lawsuit, legal action, government investigation, or regulatory action is undertaken. At the earliest recognition of a “reasonably foreseeable” matter, companies must place a hold notification directed to all potentially responsive employees. Pre-determination of notification recipients, and application of easy-to-use systems with well-documented processes, are crucial steps.

Companies must ensure that hold notifications are sent to all likely employees of potentially responsive information and records. Most companies lack the understanding of where information is located and who has access to it. In conjunction with the previous sections, an up-to-date data map of all records within an organization will enable employees and areas to be pinpointed for hold directions. Data maps break down record types within areas of the organization, physical locations, version distinction (official or non-official), and all forms of media on which information is stored.

Custodians with responsive information (including third-party vendors, providers, and storage facilities) should be pre-identified to speed up communications and increase accuracy. This is particularly important for routine or otherwise anticipated events, such as recurring types of litigation.

For unanticipated matters, companies must have the ability to quickly obtain a list of active employees, filter and create appropriate distribution lists, and communicate hold notifications to necessary contacts. By linking the records program with hold management, a company will help narrow the scope of custodians and quickly meet its compliance needs.

b. Distribute Clear Instructions

All communications should contain precise written instructions for actions that employees must take to be in compliance. Companies must ensure that expected behaviors are clearly communicated.

Employees who have, or may have, responsive material should be required to render acknowledgement of communications (as well as certification of actions). It is also important to include IT staff, and backup administrators on such communications and policies in order to coordinate preservation efforts. With a defensible, well-documented, and reliable process in place, companies will be prepared to meet possible legal obligations.

Use proven, standardized notifications to ensure clarity and consistency for hold notifications and subsequent follow-up communications. Companies need the ability to attach documents or links to
a hold notification that provides supporting information and documentation of defensible processes.

c. **Monitor Responses**
Organizations should ensure hold notification receipt and compliance by all recipients. This information may be required during the litigation or audit process. Companies must be able to demonstrate appropriate steps have been taken to ensure accurate preservation of information.

To ensure receipt and compliance, the legal hold process should require that recipients respond to confirm they have received and will comply with instructions outlined in the notification. Recipients who don’t have relevant records need to information attest to that to the Hold Administrator as well.

d. **Continuing Communications**
Companies should anticipate that employees will fail to remember previous hold obligations. Because litigation often is lengthy, companies must be able to create and schedule awareness notifications on a set frequency, and have the ability to track and manage responses automatically. Communication of hold notifications is also necessary for accurate material preservation prior to any disposal initiatives.

e. **Distribute Reminders and Awareness Notifications**
Reminders should be scheduled and distributed securely, and responses should be monitored for compliance. Reminder notices are designed to increase compliance with the hold order. If hold recipients do not respond to the original hold notice, then they should receive reminders until they comply.

f. **Process for Releasing Legal Holds**
Legal holds should be released promptly after the matter has been settled. Communication of legal hold releases should include the original hold notification, and be sent to all individuals who received the initial hold notification. Routine disposal of eligible records previously subject to the hold may be resumed. The Email Administrator should be notified that auto-deletion of email may be resumed for employees no longer part of an active legal hold, and the Backup Administrator should be notified that backups may also resume regular rotation and retention according to the Backup Policy.

In the end, it’s pretty simple. An organization needs a repeatable and defensible legal-hold process to meet legal requirements, mitigate risks, and improve efficiencies.
X. Conclusion

Developing and enforcing a corporate records management program is vastly different from simply having a "policy." Having a policy that is not consistently enforced is dangerous, as it holds the organization to a standard that is going unmet in the normal course of business.

The benefits of effectively managing corporate records are compelling:

- It’s the law.
- Privacy and records retention are quickly merging into a single issue.
- Effective records management can substantially reduce litigation costs.
- Effective records management will reduce storage costs.
- It’s an important component of your business continuity plan.

Addressing records management may seem like a daunting challenge for in-house counsel, particularly considering the rapid changes in technology and exponential growth of electronic information. But this InfoPAK will serve as a solid foundation on which to build a successful records management program.

The ACC provides several resources addressing other tenets of legal holds that are not the focus of this InfoPAK.
XII. Appendix

A. The Perfect Records Inventory

A critical component of developing a records management program that works is developing a records inventory. Knowing what records exist, where they are stored, and who owns them greatly increases the success of implementing routine disposal practices, gaining the support of employees and IT and preparing for investigations and litigation.

The Records Inventory provides the critical information companies need to execute their retention policies, clean-up legacy data and to audit compliance.

The perfect discovery map includes the following components:

- **What Records Exist.** The discovery data map should identify the types of records and information business areas work with. Orienting business people to record types produces a better discovery data map because it’s how the business people think about the information they maintain and work with.

- **Where Records Exist.** This includes knowing where records exist geographically and within the organizational structure including lines of business, functions and departments. This level of insight helps uncover areas that maintain records that shouldn’t necessarily be maintaining them. Minimizing unnecessary records and information is an easy way to cut costs during e-discovery.

- **Ownership.** The discovery data map should identify business areas that manage the official version of records and those that are maintained as copies. This will provide Legal with a roadmap allowing them to eliminate unnecessarily maintained information.

- **Media Types & Storage Locations.** Identifies what media types each area uses to manage records and the associated storage locations like hard drives, laptops, flash drives, personal email accounts, personal archives, and the supporting applications. This reveals the movement of information throughout the organization, and highlights any processes that may need to be adjusted to meet privacy or security requirements.

- **Business Processes.** The discovery data map should identify how areas move records and information within and outside of the organization. This includes third-party providers that manage and store PII on behalf of the company.

- **Retention Requirements & Practices.** Companies must know how long records are being retained across the organization to identify over retention and to set clear retention standards.
Example of a Records Inventory:

<table>
<thead>
<tr>
<th>Area</th>
<th>Version</th>
<th>Business Need</th>
<th>Area Identified Retention</th>
<th>Media</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Service</td>
<td>Copy</td>
<td>3 Years</td>
<td>Permanent</td>
<td>Email Systems</td>
<td>Archive (PST, NSF), Inbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Paper Records</td>
<td>File Cabinets / Secured/Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Electronic Files</td>
<td>Laptop Hard Drive, Workstation Hard Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Applications</td>
<td>PeopleSoft, OnPayroll, Talk</td>
</tr>
<tr>
<td>Distribution Center – Northeast</td>
<td>Copy</td>
<td>1 Year</td>
<td>1 Year</td>
<td>Email Systems</td>
<td>Inbox, Laptop Hard Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Paper Records</td>
<td>Box Warehouse</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Electronic Files</td>
<td>Workstation Hard Drive, Laptop Hard Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Shared Departmental Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PeopleSoft, OnPayroll, Virtual Edge</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Official</td>
<td>2 Years</td>
<td>7 Years</td>
<td>Email Systems</td>
<td>Archive (PST, NSF), Inbox, Workstation Hard Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Paper Records</td>
<td>File Cabinets / Secured</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Electronic Files</td>
<td>Laptop Hard Drive, My Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Applications</td>
<td>ADP, OnPayroll, PeopleSoft, Nodes</td>
</tr>
</tbody>
</table>

To develop a comprehensive Records Inventory, a company has to engage the business people. After all, they are the ones that work with the records and understand the business practices. They know the media and applications they work with and how information flows through the business. Only the business people can define the reference or business value of their records.
B. The Perfect Retention Schedule

The foundation of any corporate records management program rests on the good-faith effort to establish and enforce solid and relevant retention standards.

With a good schedule in place, companies can appropriately slash all costs and risks related to excessive storage, volumes and costs, and unnecessary litigation and investigation related collection, review and production resources. Companies are able to better control access, movement, retention and disposal of records in a professional and legally defensible manner.

The perfect retention schedule takes into account three main components:

1. **Simplicity.** The retention schedule should be simple and easy to follow. Retention schedules that are complex fail. This is not the place to document all of the applicable requirements and requirements that were considered when applying retention. Instead of confusing employees with this unnecessary information, the schedule should include:

   - **Areas:** The areas that actually have and retain the records.
   - **Record Type:** Sets the record naming standards across the organization to ensure everyone is speaking the same language.
   - **Description:** Provides an explanation and examples of what each record type includes.
   - **Retention & Authority:** Each record type should be assigned a single, clearly defined retention period and the authority that supports the retention decision. This could be based on a regulatory requirement, business need or industry best practice.
   - **Trigger:** This defines the event that starts the retention clock.

2. **A supporting Scheduling Logic.** The scheduling logic should list federal, state and federal requirements that were applied to each record type on the retention schedule. This document should capture the reasoning behind the retention periods that were applied to the retention schedule.

3. **A Records Inventory.** A Records Inventory ties the retention schedule to where records actually live, allowing employees to comply with the retention schedule easier. This also simplifies the support from the IT side. The records inventory takes into account what records exist throughout the organization, where the records are stored, the media type in which the records are stored, how long the records are kept. This information connects the dots between the retention schedule and where the information lives, so the retention schedule can be put into action.
Example of a Retention Schedule:

<table>
<thead>
<tr>
<th>Area: Human Resources</th>
<th>Record Type</th>
<th>Retention</th>
<th>Authority</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Affirmative Action Files</strong></td>
<td>2 Years</td>
<td>29 CFR 1620.32</td>
<td>Closed</td>
</tr>
<tr>
<td></td>
<td><em>Includes job descriptions and work force analysis.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Benefit Folder</strong></td>
<td>6 Years</td>
<td>29 USC 1027</td>
<td>Closed</td>
</tr>
<tr>
<td></td>
<td><em>Official documentation for employees’ enrollment in medical, insurance and 401K plans. Includes beneficiary cards, designation records, outplacement benefit notices, statements of health benefits, contributions, cobra records, etc.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Disability Records</strong></td>
<td>6 Years</td>
<td>29 USC 1027</td>
<td>Date of Claim</td>
</tr>
<tr>
<td></td>
<td><em>Includes short-term and long-term disability.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Drug Screening Records</strong></td>
<td>3 Years</td>
<td>29 CFR 1627.3</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td><em>Includes testing results and reporting.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EEO Compliance Records</strong></td>
<td>10 Years</td>
<td>Legal Consideration</td>
<td>Calendar Year</td>
</tr>
<tr>
<td></td>
<td><em>EEO-1, EEO-2 and annual affirmative action reports.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Medical Files</strong></td>
<td>5 Years</td>
<td>29 CFR 1904</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td><em>Includes medical records, doctor notes, authorization for treatment.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Payroll Records</strong></td>
<td>8 Years</td>
<td>State Payroll</td>
<td>Calendar Year</td>
</tr>
<tr>
<td></td>
<td><em>Payroll changes, check registers, deductions, earning reports, attendance records, time sheets, incentive awards, reconciliations, reports, etc.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Personnel Files</strong></td>
<td>8 Years</td>
<td>State Payroll</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td><em>Personnel files including employee reviews, appraisals, disciplinary actions, status changes, compensation agreements, employee agreements, non-disclosure agreements, non-compete records, exit interviews, etc.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To develop a comprehensive records inventory, a company has to engage the business people. After all, they are the ones that work with the records and understand the business practices. They know the media and applications they work with and how information flows through the business. Only the business people can define the reference or business value of their records.

The retention schedule is the basis for a successful records program, and for disposal of records. Its accuracy is important to ensure information is maintained no shorter or longer than the appropriate time period. The false security of an extensive and complex retention schedule is one of the biggest problems in records program enforcement. It causes confusion with employees and IT and results in records and information being retained beyond requirements.
C. The Perfect Discovery Data Map

Up-to-date knowledge of all data repositories and its owners is a key component to a defensible e-discovery process. Knowing what records exist, where they are stored, and who owns them will increase the effectiveness and efficiency of the e-discovery process. A Discovery Data Map provides deep insight into the electronic applications that employees use and control. It serves to identify all the locations within the corporation where potentially relevant data may be stored.

Not only does the Discovery Data Map improve the pre-litigation preparation, but it also highlights potential risks allowing the company to eliminate unnecessary or redundantly retained records.

The e-discovery industry is a $6 billion dollar industry for a reason. The companies that keep everything really feel the pain during discovery and specifically during the review process. The easiest way to impact discovery and review costs is by eliminating unnecessary records.

The perfect discovery map includes the following components:

- **What Records Exist.** The discovery data map should identify the types of records and information business areas work with. Orienting business people to record types produces a better discovery data map because it’ how the business people think about the information they maintain and work with.

- **Where Records Exist.** This includes knowing where records exist geographically and within the organizational structure including lines of business, functions and departments. This level of insight helps uncover areas that maintain records that shouldn’t necessarily be maintaining them. Minimizing unnecessary records and information is an easy way to cut costs during e-discovery.

- **Ownership.** The discovery data map should identify business areas that manage the official version of records and those that are maintained as copies. This will provide Legal with a roadmap allowing them to eliminate unnecessarily maintained information.

- **Media Types & Storage Locations.** Identifies what media types each area uses to manage records and the associated storage locations like hard drives, laptops, flash drives, personal email accounts, personal archives, and the supporting applications. This reveals the movement of information throughout the organization, and highlights any processes that may need to be adjusted to meet privacy or security requirements.

- **Business Processes.** The discovery data map should identify how areas move records and information within and outside of the organization. This includes third-party providers that manage and store PII on behalf of the company.

- **Retention Requirements & Practices.** Companies must know how long records are being retained across the organization to identify over retention and to set clear retention standards.
Example of a Discovery Data Map:

To develop a comprehensive Discovery Data Map, a company has to engage the business people. After all, they are the ones that work with the records and understand the business practices. They know the media and applications they work with and how information flows through the business. Only the business people can define the reference or business value of their records.
D. The Perfect Personal Data Inventory

Companies that are serious about preventing privacy breaches and complying with privacy laws must develop a personal data inventory that uncovers how employees use, manage, store and share sensitive and personally identifiable information. The only way to accomplish this is to develop a personal data inventory with direct input from business people.

Many breaches, perhaps most breaches can be avoided by developing a detailed Personal data inventory and to understand where and how personal data is managed and consequently exposed. Quite simply, companies cannot possibly protect personal information without knowing where the organization’s personal information is, which includes both within the organization and at service providers and any of their service providers.

The perfect personal data inventory includes these main components:

- **What Records Exist.** The personal data inventory should identify the types of records and information business areas work with. Orienting business people to record types produces a better PDI because it’s how the business people think about their information.

- **Where Records Exist.** This includes knowing where records exist geographically and within the organizational structure including lines of business, functions and departments. This level of insight helps uncover areas that have PII that don’t necessarily need it. Minimizing unnecessary records and information with PII is an easy way to reduce privacy breach risks.

- **Media Types & Storage Locations.** Identify what media types each area uses to manage records and the associated storage locations like hard drives, laptops, flash drives, personal email accounts, personal archives, and the supporting applications. This reveals the movement of information throughout the organization, and highlights any processes that may need to be adjusted to meet privacy or security requirements.

- **Specific PII Elements.** For each record type within each area the specific elements of PII should be identified. A mistake, companies often make is to only ask business people to apply data classifications to their record types. Data classifications become subjective labels as opposed to identifying concrete elements like social security numbers or mother’s maiden name.

- Data classifications, while useful, provide no real utility in evaluating compliance with privacy laws. Laws provide definitions of covered information based on combinations of specific elements. Unless a company includes these discrete elements in a personal data inventory, the compliance with changing privacy laws can’t be evaluated.

- **Business Processes.** The personal data inventory should identify how areas move records and information within and outside of the organization. This includes third-party providers that manage and store PII on behalf of the company.

- **Retention Requirements & Practices.** Companies must know how long records containing PII are being retained across the organization to identify over retention and
to set clear retention standards. Many privacy laws are now setting maximum retention periods for PII. This is forcing companies to move away from the archaic retention practices traditionally implemented in the United States where retention requirements were considered “minimum” periods. Most companies are shifting to the more appropriate international position that retention requirements are “maximum” periods and that records must be immediately disposed of after obligations are met.

**Example of a Personal Data Inventory:**

<table>
<thead>
<tr>
<th>Employment Records</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td><strong>Business Need</strong></td>
</tr>
<tr>
<td>Customer Service</td>
<td>3 Years</td>
</tr>
<tr>
<td>Human Resources</td>
<td>6 Years</td>
</tr>
</tbody>
</table>

- **Media:** Email Systems, Flash Drive, Local hard drive, PST / Archive
- **Paper Records:** Company Cabinets, Department Cabinets

<table>
<thead>
<tr>
<th>Employment Records</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td><strong>Business Need</strong></td>
</tr>
<tr>
<td>Human Resources</td>
<td>6 Years</td>
</tr>
</tbody>
</table>

- **Media:** Electronic Files, Laptop Hard Drive, My Documents, Shared Departmental Drive, Workstations Hard Drive
- **Email Systems:** Inbox, Local hard drive, Other, Printed and filed, PST / Archive
- **Applications:** Adobe Creative Suite, Solidworks
- **Paper Records:** Department Cabinets

<table>
<thead>
<tr>
<th>FMLA / Requests</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td><strong>Business Need</strong></td>
</tr>
<tr>
<td>Human Resources</td>
<td>3 Years</td>
</tr>
</tbody>
</table>

- **Media:** Electronic Files, Shared Departmental Drive

<table>
<thead>
<tr>
<th>Personal and Sensitive Categories</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PII</strong> = Personally identifiable information</td>
<td><strong>SI</strong> = Sensitive Information (EU)</td>
</tr>
<tr>
<td><strong>PHI</strong> = Patient Health Info.</td>
<td><strong>CCI</strong> = Corporate Confidential</td>
</tr>
<tr>
<td><strong>FIN</strong> = Financial Information</td>
<td><strong>IP</strong> = Intellectual Property</td>
</tr>
</tbody>
</table>

To develop a comprehensive personal data inventory, a company has to engage the business people. After all, they are really the only ones that know what records and information they have and use, the specific sensitive and valuation elements they contain, how long they retain it, and what they are doing with the information.

The personal data inventory provides the key insights needed to streamline information management practices, uncover privacy vulnerabilities and to meet privacy objectives and comply with laws.
XII. About Jordan Lawrence

For 24 years, Jordan Lawrence has been helping companies to develop, implement and enforce defensible records retention schedules and policies and comply with privacy requirements.

We are an Alliance Partner with the Association of Corporate Counsel and have extensive experience working with companies of all size and industry including; AVIS, E-Trade, Fossil, Newell Rubbermaid and Stanley Black & Decker. We leverage this experience in many ways including unique industry best practice and benchmark standards.

Contributor’s Biographies:

Alice Lawrence, Principal, Jordan Lawrence

Alice Lawrence is a Principal of Jordan Lawrence, a leading solution provider for records retention, data privacy and information governance. She has over 20 years of experience in information technology and governance and is responsible for the executive strategies and implementation process necessary to connect policy to practice.

Alice joined Jordan Lawrence in 1990 and advises in-house counsel, compliance and privacy professionals in the areas of records management, data privacy and e-discovery. She plays a key role in the development of technology that helps companies develop effective, defensible and cost effective information governance programs that address information across all platforms and media. Most recently, she was the driving force in the development of the company’s Assessment for Records Risks™, which is the basis for the recognition by Gartner, Inc. as a Cool Vendor in Risk Management, Privacy and Compliance, 2011.

She is a Certified Information Privacy Professional (CIPP) and frequent contributor and speaker in the legal, IT and privacy communities on managing records to mitigate risks.

Marty Provin, Executive Vice President, Jordan Lawrence

Marty Provin is Executive Vice President of Jordan Lawrence, a leading solution provider for records retention, data privacy and information governance. He has over 20 years of experience in information technology and governance.

Marty joined Jordan Lawrence in 2003 and advises in-house counsel, compliance and privacy professionals in the areas of records management, data privacy and e-discovery and the confluence of technology in these areas. He plays a key role in helping companies develop effective, defensible and cost effective information governance programs that address information across all platforms and media. He is a Certified Information Privacy Professional (CIPP) and frequent contributor and speaker in the legal and privacy communities. Most recently he was a featured speaker at the 2011 Twin Cities Privacy Retreat, 2011 Secure World Expos, and the 2011 IAPP Privacy Academy.
Prior to joining Jordan Lawrence in 2003, Marty spent 13 years in the technology industry where he worked with Fortune 500 Companies in developing solutions to manage workflow and increase efficiency.

Rebecca Perry, Executive Vice President, Jordan Lawrence

Rebecca Perry is Executive Vice President of Jordan Lawrence, a leading solution provider for records retention, data privacy and information governance. She has over 19 years of experience in records management and information governance.

Rebecca advises in-house counsel, compliance and privacy professionals in the areas of records management, data privacy and e-discovery and the confluence of technology in these areas. She plays a key role in the success and oversight of developing and enforcing effective, defensible and cost effective information governance programs that address information across all platforms and media.

She is a Certified Information Privacy Professional (CIPP/US/G) and frequent contributor and speaker in the legal and privacy communities. Most recently she was a featured speaker on a series of industry webinars covering topics on privacy, SharePoint, and retention program development.
XIII. Endnotes

1 La Ley Federal de Protección de Datos Personales en posesión de los particulares
3 Jordan Lawrence Group – *Over-Retention of Records*
4 Jordan Lawrence Group – *Records Management Primer*, available at
6 Jordan Lawrence Group – *Volume Correction Strategies for Email*
10 Jordan Lawrence Group – *Volume Correction Strategies for File Shares*

16 Jordan Lawrence Group – *Volume Correction Strategies for Paper Records*