



Boston Concord Hanover Manchester



James P. Harris
Direct dial: 603.627.8152
Fax: 603.641.8731
jharris@sheehan.com

Practice Areas

Corporate Law and Governance
Intellectual Property and
Technology
Private Companies and
Professional Practices

Additional information for this attorney
may be found on our website.

Good Company

Record Retention in an Increasingly Paperless World

Wednesday, June 29, 2011

The first question usually posed by companies interested in crafting information retention/destruction policies is "How long should we keep this stuff?" There is, however, a more fundamental question that must be answered first and that is "Should we keep all this stuff?" Most companies have already determined that it is wise to discard or delete information and they want to create a policy memorializing and standardizing that practice. Companies should step back, however, and perform the following self-analysis first before focusing on what information to discard and when to discard it.

Written information retention/destruction plans serve both business and legal reasons. These plans help companies remain organized and efficient as irrelevant or stale information is discarded making it easier to find relevant and pertinent information. Reducing the volume of information reduces storage costs both in terms of physical space and computer hardware. Reducing the quantity of business records also tends to reduce litigation costs because less time is spent culling out records relevant to the dispute. Thanks to recent changes to the rules of civil procedure, companies who discard information pursuant to a written plan before they reasonably anticipated litigation cannot be sanctioned for having done so. Those rule changes are a double-edge sword, though. Discarding information without a written retention plan or failing to comply with the written plan creates the risk of severe sanctions from a court. The possible sanctions range from monetary sanctions to dismissal of a party's claims or defenses. These factors lead companies to conclude that a well-crafted information retention/destruction policy is essential in today's marketplace.

Before one sets pen to paper, or fingers to keyboard, to draft an information retention/destruction plan, companies should put themselves through the following worst-case-scenario fact pattern and evaluate how their company would likely fare under the circumstances. Assume that your company has adopted an information retention/destruction plan that calls for all employees to delete drafts of documents (so the company retains only final versions of word documents, for example) and to delete all emails sent or received more than one year ago. The implementation of the policy is not automated, so the company relies upon each employee to delete documents and emails according to this schedule. The sheriff arrives to serve a lawsuit (the nature of the allegations are not important for purposes of this exercise). The company then begins to gather information relevant to the claims and defenses. The company realizes that implementation of the information retention/destruction plan has not been uniform across the company. Some employees adhered to the plan, so they deleted drafts of documents and old emails. Other employees kept drafts and archived all emails. The result is that some (but not all) drafts of documents persist and some (but not all) emails remain.



Three months into the litigation, the company's opponent learns that some (but not all) information was discarded. The opponent has reviewed the company's written information retention/destruction plan and has concluded that it was not implemented uniformly. To the opponent, the absence of some documents and emails is suspicious. The opponent argues to the court that those selected documents that were discarded were the most important to the litigation. The opponent alleges that the selective deletion was part of a plot to delete information harmful to the company and beneficial to the opponent's claims. The opponent now moves the court for sanctions against the company for failing to preserve crucial information.

This hypothetical plays out in courtrooms each day. Company resources are spent, not on the merits of the case itself, but rather on whether one party failed to preserve information, most of which probably is not central to the litigation. The selective loss of data, however, is suspicious and courts view improper discarding of data as an affront to the judicial process. Having a written information retention/destruction plan is fine so long as it is implemented uniformly. Otherwise, companies merely set standards by which their conduct will be judged and prepare to be hoisted by their own petard.

The most important inquiry for companies looking to adopt information retention/destruction policies is whether they believe it will be implemented unvaryingly. Answering this question requires an analysis of the workplace culture and the psychology of the employees. Most people tend to be pack rats, particularly with respect to electronic data. If it will be a constant struggle to overcome those natural tendencies, establishing a policy with short time periods or differing time periods for different types of information is unwise. It would be advisable instead to select longer periods that can be applied to large categories of information making compliance easier. Companies also need to examine whether they want to be in the position of policing employees' compliance with the policy, including disciplining employees for non-compliance. Companies should consider whether they want to create an atmosphere where they monitor employees' email accounts to ensure that stale emails are deleted according to the policy, for example. Because information retention/destruction policies permeate to every business record and therefore every act performed by company employees, these policies should be adopted only after a thoughtful analysis of the effect they will have on company culture. Selective implementation by rank and file employees completely erodes the business and legal justifications for having an information retention/destruction policy.

Another important question to address is to what extent the company can automate the discarding or deleting of information. The greater level of discretion afforded to employees, the greater chance of inconsistent implementation. These policies put employees in the position of determining whether a particular document should be deleted in 1 year or 7 years (whether it falls within Category A or Category B), for example. Employees might be relied upon to take time out of their work days to delete information, which most employees will view as a task that interferes with rather than enhances their productivity. Companies should examine their resources to determine to what extent can these decisions be removed from the employees and be automated. Can email systems be set up so that emails are automatically purged, for example? Automation increases the chances of uniform implementation thereby increasing the chances that the policy will serve its purpose.

Companies should also address the philosophical question of whether they want to be in the position of having all information relevant to a dispute or whether they are comfortable with gaps in the information. Some claims might not be filed for several years after the events underlying the claims took place. Employees who worked on a particular file may have left the company taking a knowledge base with them. Companies should decide whether they want to be able to recreate past events through the information in their files. This might be particularly true for companies whose main "product" is their judgment or analysis. Keep in mind that your opponent might be a pack rat, so the opponent might have every draft of every document and every email between the parties. Whether harmful or helpful, sometimes being able to recreate an accurate picture of events that occurred several years before may have its own inherent value to the company.

Do not misconstrue the purpose of this article. The conclusion of this piece is **not** "Thou shalt keep everything." There are substantial benefits to deleting and discarding information according to a set schedule. The benefits

SHEEHAN
PHINNEY
BASS +
GREEN PA



ATTORNEYS AT LAW



Boston

Concord

Hanover

Manchester

include saving money on storage costs and reducing litigation costs if it becomes necessary to review the now smaller universe of available information. This article, rather, asks companies not to skip ahead to “How long should we keep this stuff?” Instead, companies should first ask themselves “Should we keep this stuff?” Do not automatically assume that it is wise to discard and delete without first examining the benefits and potential pitfalls. The costs of electronic storage decrease over time and will continue to decrease. If companies are organized in the way in which they store their data, the costs of trying to find particular pieces of information should be minimized. Moreover, the costs to automate searches of electronically stored information will also continue to decrease over time. Regardless of whether a decision is made to tend to save or to tend to delete, these overarching questions should be answered first so that a written policy can be crafted to match the company’s philosophical decisions.

This article is intended to serve as a summary of the issues outlined herein. While it may include some general guidance, it is not intended as, nor is it a substitute for, legal advice. Your receipt of Good Company or any of its individual articles does not create an attorney-client relationship between you and Sheehan Phinney Bass + Green or the Sheehan Phinney Capitol Group. The opinions expressed in Good Company are those of the authors of the specific articles.

Additional information for this attorney
may be found on our website.

SHEEHAN PHINNEY BASS + GREEN PA
www.sheehan.com

Manchester, NH | Concord, NH | Hanover, NH | Boston, MA
800-625-SPBG (7724)