PO Box 3146
Alpharetta, GA 30023
(770) 951-2080
www.cyberscrub.com

Data Destruction and Document Life Cycle Policies: Considerations for Compliance with Federal Mandates and Acts

A perspective on issues relating to Electronic Data Retention and how this relates to compliance with federal and state regulations such as Sarbanes-Oxley, HIPAA, FACTA, Gramm-Leach-Bliley (GLB) and others.

All of the above listed statutes, in one way or another mandate the secure, non-recoverable destruction of data. Examples would be protected health information (PHI), customer data, financial transactions, email, instant messaging and more.

It is a given that utilizing the standard delete key on a computer keyboard does not destroy the data. “Deleted” data is recoverable. It is essential to utilize methods that securely erase data beyond any type of forensic recovery. The preferred method is utilizing software that overwrites the data until the existing file(s) is obliterated. The significant benefit of overwriting or “wiping” data” is that the process is verifiable and can produce a detailed and auditable log file to document the procedure.

Most organizations have to this point limited such data destruction to the sanitization of computer hard drives designated for disposal or redeployment. However, total disk destruction does not address the myriad of information that resides on your *active* computers. This is particularly relevant, but often overlooked.

To further illustrate, consider the reality of years of data residing on individual client machines. Even if these computers are regularly purged of outdated records, two problems remain:

1) The user must be disciplined to expunge obsolete data. In a practical sense, this is not feasible; users will simply adjust this task to their schedule or perform it erratically at best. Furthermore, such *ad-hoc* methods could lead a litigant to contend that such action was initiated *in response to an investigation*- culminating in charges of obstruction of justice.

2) A more serious problem lies in the fact that any data the user deletes is, in almost all cases, recoverable. So in essence, this time intensive effort is for naught. Even with the best of intentions, the data is destroyed in a hap-hazard, subjective manner. This process, or lack thereof, is a grenade waiting to explode.

Ideally the entire data destruction process should be policy driven, automatic, transparent, stealth and passive.

An automated process can enforce established policies. It is not dependent on user activation. It takes place in the background, unobtrusively. It is passive and requires no user intervention. Most importantly, the incorporation of sophisticated data wiping would render the targeted records non-recoverable.

In the absence of a clear, policy-driven, automated and documented process for the secure erasure of information *the entire exercise is subjective*- and this is where the true liability and danger lies.

Let us examine a few examples of the result of non-disciplined e-destruction:
In *Residential Funding Corp V. DeGeorge Financial Corporation*, a 2002 federal case in the New York Second Circuit Court of Appeals, the plaintiff won a $94.4 million jury verdict even though the email that was not produced was deemed to have little value. The plaintiff asserted that delay and destruction were sanctionable, and the court agreed. If the outdated email had been automatically destroyed *as a matter of policy*, DeGeorge would have been able to counter successfully that they could not produce what they did not possess.

It is essential to retain designated data, but it is just as essential to destroy data you no longer need. Establish an electronic records policy and stick to it. They can't subpoena what you don't have.

Other cases abound- Wall Street behemoth Morgan Stanley recently settled an email case for $15 million- that's enough to get anyone fired. In essence, Morgan Stanley had to settle a lawsuit with the FTC for not producing tens of thousands of email messages during probes of Wall Street analysts and others from 2000 to 2005.

Now, let's look at the other side of the coin- *keeping everything:*

In 2004 Microsoft turned over 500,000 emails from 60 employees. You can be sure a wealth of information was gathered from this action that had nothing to do with the initial request. Such disclosure not only produces valuable intelligence to competitors, but can expose your organization to charges of criminal activity not originally conceived by prosecutors.

In yet another instance financial services giant ING emails revealed that the firm allowed some of its clients to engage in extensive "market timing" which is a potentially abusive trading practice at best, as early as 2001.

Despite these highly publicized cases involving email **only 35%** of companies even have email retention policies. Most companies are literally sitting ducks. Computer data is the electronic equivalent of DNA.

Now let us examine the federal requirements for the destruction of electronic data.
Remember, in almost all cases this data resides on active, in service computers. And consider this salient point: How are you enforcing destruction and document life cycle policies when that data resides in multiple local computers and repositories?

The Fair Credit and Accurate Transactions Act (FACTA)

Almost any type of business that handles customer transactions is subject to this federal regulation. It is meant to address the dangers of identity fraud and other potential consumer liabilities. In practical terms, this means the destruction of customer information, paper or electronic, at the appropriate time.

Sarbanes-Oxley Act
Companies have the task of destroying valueless documents while retaining those relevant to audits and investigations. As mentioned earlier, *ad-hoc* or inconsistent destruction heightens the risk of liability under Sarbanes-Oxley.

Health Insurance Portability and Accountability Act (HIPAA)
This concerns everyone- Privileged health Information (PHI). Severe penalties and fines may be imposed for the improper stewardship of these sensitive records. Some patient records will outlive their usefulness in days, others in years, but all will require destruction at some point.

The Harvard University Records Destruction Policy is excellent. Four bullet points say it all:

Records may only be destroyed if:

- *All retention periods have expired*
- *All audit requirements have been satisfied*
- *There are no pending requests for information and*
- *There is no foreseeable litigation involving the records*

Once this criteria has been met the data should be destroyed

Companies should consider forming a *Compliance Task Force* and create detailed logs of record purging and destruction activities. Every organization should be prepared to meet the challenges posed by the demands of data discovery. By having a suitable electronic document retention policy in place, *and being able to prove this policy has been implemented,* you will be prepared for unseen challenges.

In summation, you should be able to demonstrate to the court these critical points:
1) The existence of a comprehensive retention policy, and
2) That it entails rigorously enforced penalties for non-compliance.

This will limit and curtail the exposure and liability of your organization from a potentially ruinous criminal prosecution for obstruction of justice or other litigation.