



**Document Destruction: An Essential Part of Your Record Retention Program**

By: Jonathan Stanley  
May 9, 2008

Most companies have already recognized the importance of a comprehensive record retention program. Record retention programs set forth in advance a schedule for how long certain categories of documents should be preserved. If a document is disposed of pursuant to a record retention program that is properly implemented and consistently observed, courts will normally not sanction a company or allow unfavorable conclusions to be drawn if that the document is subsequently unavailable for discovery in litigation. However, even when companies faithfully follow their record retention programs, they may run unnecessary legal risks if they do not monitor what happens to the documents they elect not to retain.

The federal government and an increasing number of states are responding to concerns about identity theft by passing laws requiring businesses to protect the confidential information of their customers. These laws can be violated by carelessly disposing of documents, and authorities have taken meaningful action against violators. In a recent case, drugstore giant CVS was recently ordered to pay \$315,000 by a Texas court after it was discovered that hundreds of its customer records were dumped behind one of its facilities.

These risks can be managed by implementing a document destruction policy as a part of an existing record retention program. Document destruction policies may be tailored to fit the needs of individual businesses, but the goal of every policy should be to render documents that contain consumer personal information or other sensitive information unreadable before they are allowed to leave the custody of the company. For paper records, this goal can be achieved by shredding, burning or



## Document Destruction

pulverizing. If a business disposes of a relatively small amount of paper records, it may make sense to institute a blanket policy that all documents to be disposed of must be destroyed, regardless of their content, before they leave the premises. If a business generates voluminous amount of paper records and only a small portion of these records contain personal or other sensitive information, it may be more cost effective to institute a policy that requires only that certain specified types of documents be destroyed.

For electronic records, every company should have a policy requiring that all data be removed from old computers and portable storage devices using a wipe utility program before they leave the company premises. Deleting files using the keyboard or mouse commands usually isn't sufficient because files may continue to exist on the computer's hard drive and could be retrieved easily.

No matter what policy a company chooses to implement, it is essential that management convey to employees the importance of compliance with the policy. Every new employee should be asked to sign an agreement to follow the company's document disposal policy. Make shredders or other destruction devices available and post reminders in areas where sensitive information is often disposed of, such as by copy machines, as well as where employees congregate. Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices. H<sup>3</sup>GM is available to assist its clients in developing a document destruction policy that meets their individual needs