



# THE INFORMATION MANAGEMENT DIGEST

*Our Business, Is Keeping Your Business - Your Business!*

A Service of WesTex Document, Inc.

April 2011

## MAINTAINING A CHAIN OF CUSTODY FOR CONFIDENTIAL INFORMATION

In the current environment of HIPAA, Gramm Leach Bliley and other privacy litigation, organizations that handle sensitive information must pay close attention to procedures for creating, using, storing and disposing of that information. Organizations are very accustomed to thinking of information in terms of authorized access during its stages of creation and active use. Personnel records, payroll information or sensitive financial records of the organization are maintained in a more secure area. Likewise, computer backup tapes or other emergency restoration media may be kept under lock and key. In both examples, access to the information is limited to those who are authorized to view or use the information. In addition, when archived information is moved off-site in order to save money, only a limited number of persons can order information retrieved and delivered back to the organization. This limited group of requesters is maintained on a "authorization list." Other employees of the company are not permitted to request information until they are added to the list. When information progresses from its storage to its destruction phase, the same care and handling is required.

Your organization may dispose of confidential information at intervals that may vary from large annual purges of data to daily pick-ups. No matter how often confidential data is prepared for destruction, care must be taken that someone has assumed possession of the confidential informa-



tion from the point that it leaves a secure area until the time it is destroyed. This span of time, and the series of events that take place in order to document responsibility for the confidential information, is known as a "chain of custody."

Chain of custody is a term used in the management of legal evidence. While it may seem extreme to compare records or confidential trash with bullet casings or fingerprints collected at a crime scene, the concept is the same. The ARMA Glossary of Terms defines a record as "*Recorded information, regardless of medium or characteristics, made or received by an organization that is **evidence** of its operations, and has value requiring its retention for a specific period of time.*"

Business records are admissible as evidence in court, as well, so “chain of custody” seems to be a very appropriate description.

## **Security Begins at Home**

If confidential or sensitive information is being produced or used by the organization, an appraisal of information security policies, procedures and practices should be undertaken on a periodic basis. This may take the form of a compliance audit, or remedial training. In a compliance audit format, information security protocols such as authorization lists, security procedures for sensitive or confidential records, password authentication procedures, and additional physical office security such as card readers, key pads, biometric entries and CCTV camera networks should be verified as working properly. In addition, audits of waste paper and secure destruction containers should also be conducted in order to make sure that confidential information is not making its way into the solid waste stream, and solid waste is not being shredded unnecessarily. Remedial training of staff should take place at least once a year and after each new hire. Proper information handling procedures should be carefully reviewed, including a review of the difference between a locked, secure destruction container and a trash receptacle.

## **Chain of Custody and Quality Procedures**

The chain of custody begins by ensuring that secure destruction bins or information to be purged remains in secure areas until it is collected for destruction. Following identification of the information to be destroyed, a uniformed employee of your confidential destruction partner arrives at your location, presents his identification and begins to collect the information to be destroyed. Some type of documentation bearing a signature or other unique identifier is an excellent method of demonstrating the transfer of information from your facility to the destruction vehicle. If a mobile vehicle is used, employees may be on hand to witness the destruction of confidential information. If the information is being transferred to a secure destruction facility, care should be taken that the information is transferred in an enclosed, locked vehicle.

While in transit, vehicles may be tracked using active or passive GPS systems. This provides your confidential destruction partner with data regarding each stop made, the time in transit, vehicle speed and other information. Upon the arrival of the vehicle at the secure destruction facility, items contained in locked bins, or in bags if your facility uses consoles, are off-loaded to the shredding facility for destruction. When the information has been shredded, you should be notified. If the materials to be destroyed were official records of your organization, a certificate of destruction should be issued to you in order to confirm the deletion of the confidential information. When you are notified of the destruction or when you are issued a certificate of destruction, this completes the custody chain.

### **Tips for Managing Your Chain of Custody**

- Do you have good facility security?
- Are sensitive areas or document storage devices kept locked?
- Are authorization lists and passwords periodically updated?
- Are new hires trained in secure information policies, including the use of confidential destruction containers?
- Are secure destruction vendor employees uniformed and presenting company identification?
- Are confidential destruction bins kept locked until changed by your secure destruction vendor?
- Are destruction vehicles locked, except when employees are physically present?
- Is confidential information destroyed quickly and completely?
- Is a certificate of destruction provided following the destruction of official records?

# What Should be on a Certificate of Destruction?

Official record copies with a limited retention period will eventually reach their disposition date. Following the preparation of a disposition report which should be reviewed by departments in order to ensure the records are not needed for litigation, audit or other purposes, the official record copies can then be destroyed. Should there be future litigation, some evidence of the official destruction of these records should be provided. This is the purpose of a certificate of destruction.

A destruction certificate is a form, or in some cases a letter, that contains basic information about the official records that were destroyed. The certificate should list the name and contact information of the records owner, descriptive

information regarding records series, date ranges, or other significant tracking information of the records that were destroyed, the total volume of records destroyed, the means used to destroy the records, the name of the company performing the destruction, the signature of the secure destruction company representative and the date the destruction took place. Some certificates of destruction may contain even more information such as a list of authorizing signatures of departments that have reviewed the disposition list, etc.

While individual cartons may be listed, it is usually possible to group records by a relevant range. If this is the case, then these ranges can be noted on the certificate.

---

## Information Management in the News

### SAVING OUR DATA FROM DIGITAL DECAY

An old-school alternative to digital storage has a modern spin that could save us from future information loss as technology changes and today's state of the art devices become tomorrow's museum pieces. Link: <http://www.sciencedaily.com/releases/2010/11/101116072749.htm>

### IS SaaS FOR DOCUMENT IMAGING HERE TO STAY?

I recently read that "in 5 years 75% of document imaging will be SaaS based". I don't think it will take that long. Participating in recent "ECM conventions" and listening to how (not what) vendors are speaking and positioning their products and solutions, I realized that SaaS is top of mind for "our customers" in the ECM space. Link: [http://growyourbiz.kodak.com/post/?id=5203571190647727897&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+kodak%2Fgrowyourbiz+%28Grow+Your+Biz+is+a+blog+about+Kodak+products+and+services+in+the+graphic+communications+business.%29](http://growyourbiz.kodak.com/post/?id=5203571190647727897&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+kodak%2Fgrowyourbiz+%28Grow+Your+Biz+is+a+blog+about+Kodak+products+and+services+in+the+graphic+communications+business.%29)

### CLOUD DATA PROTECTION NECESSARY, ATTAINABLE

November 17, 2010 – Access control rules, strong authentication and best-of-breed network security infrastructure topped the list for cloud requirements in a new survey on cloud security conducted by Hubspan, a provider of cloud-based business integration services. A majority of respondents (84 percent) agree that sensitive data can be safely stored in the cloud. Link:

<http://www.information-management.com/news/cloud-data-protection-necessary-attainable-10019139-1.html>

Related Link:

[http://www.itnews.com.au/promos/interstitial/interstitial2.html?l=10;H13cX2uk71UuxvArnTIukmg63H2TZzy7161SyEKnqqazpTQvaE;20101123\\_ITN\\_VMWare\\_Nov](http://www.itnews.com.au/promos/interstitial/interstitial2.html?l=10;H13cX2uk71UuxvArnTIukmg63H2TZzy7161SyEKnqqazpTQvaE;20101123_ITN_VMWare_Nov)

### MOST COMPANIES NOT ERASING SENSITIVE DATA

Most businesses don't properly erase sensitive data from old computers and hard drives, leaving them highly susceptible to data breaches, according to a survey by Kroll Ontrack. Only 49 percent of more than 1,500 respondents polled worldwide say their businesses are systematically deploying a data eraser method. Among that group, 75 percent don't delete data securely, according to Kroll. Link:

<http://www.complianceweek.com/blog/aguilar/2010/11/16/most-companies-dont-erase-sensitive-data-risking-breaches/>

## New Holocaust Archives Unveiled

New artifacts of the Holocaust were unveiled at an event in January at the Kopolow Building in St. Louis, Missouri. Documents, photos, diaries, and other items from Hitler's Germany and its neighbors were shown for the first time in honor of the January 27 International Holocaust Remembrance Day. According to a *Jewish Light* article, the artifacts included letters from the concentration camps, Nuremberg trial documents, and several photographs of the horrifying events that took place during the Holocaust.

Jewish archivist Diane Everman said, "If you are familiar with some of the items in the Holocaust Museum, that is literally the tip of the iceberg." Everman continued, "There is so much more, everything from manuscripts materials to photographs to oral histories, material culture items that add depth to what is already in the museum."

The letters unveiled at the Museum were mostly letters from people in Germany that were becoming aware of the Nazis plans and were in need of escape. "There are letters writing to relatives or even complete strangers because they needed a sponsor, they needed money, they needed assistance to get out," said Everman. "The response was often, 'I'm sorry, I can't. I'm already sponsoring X number of people. I can't do one more.' We also had family members, even far-removed distant cousins, who did help people get out."

The article said that documents of the Nuremberg trials were also displayed in the archive. Two collections from St. Louis area residents Hedy Epstein and the late Whitney Harris were included in the materials. "Even though a lot

of it is available elsewhere, at least with Hedy and Whitney, there are other things, including an oral interview with Hedy and all kinds of additional information," Everman said. "So if somebody is interested in doing research on that aspect of the post-war period and the trials those collections are just invaluable."

New visual archives were also unveiled at the museum. Photographic work by liberators displayed the types of scenes they were exposed to upon coming into the camps. "They show what they saw, what they experienced," she said. "That's a huge part of the photographic collection."

According to the article, objects that were commemorative of Hitler's forces to push the message of National Socialism were revealed. Collectible cigarette packages consisting of photos on thin paper were shown. The pictures depict everything from the 1936 Berlin Olympics to Hitler in formal wear to troop movements. The idea seems to have been similar to collecting baseball cards in America. Hitler Youth documents to diaries, to day planners, to cantina money from Buchenwald, were displayed as well.

The article noted that the material was gathered from concentration camps, communities in the United States, Denmark, Sweden, and other countries where Jews sought refuge. Artifacts were also gathered from Jewish refugees that escaped to China. "Those are really interesting. I honestly didn't know much about the Jewish community in Shanghai before the war but these collections have photographs, people's diaries and letters back home about what life was like there, even the restaurants that were open and the theater groups that existed," Everman said.

The archives can be seen at the Kopolow Building in St. Louis.



## WesTex Document, Inc.

815 S. Gilbert Drive  
Reese Science & Technology Center  
Lubbock, TX 79416

CALL (806) 885-2906 or visit our web <http://www.westexdocument.com>

### ARCHIVE - IMAGING - DESTRUCTION SERVICES

West Texas's most trusted source for meeting your record management needs. We offer professional storage, digital imaging and secure destruction of any type of records you may have. We can shred material to three different particle sizes - no strip cutting used; we can send two mobile trucks that will destroy up to 7 TON an hour between them; we can image and copy (printing) documents up to 24 x 48"; professional record archive services and consulting for all of your professional RIM needs. Call or come visit us to learn more and tell us how we might help you.

Lubbock Chamber Member Since 1997

ISO 17799:2005 (Information Security) Compliant

**OUR BUSINESS, IS KEEPING YOUR BUSINESS - YOUR BUSINESS!**

