



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 offsite 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 information 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.

SARBANES OXLEY AND ELECTRONIC RECORDS

The Sarbanes-Oxley Act (SOX) was passed by the United States Congress and signed into law by President Bush in 2002. This law was passed in response to Enron, World Com and other corporate governance and financial scandals. The Act established a Public Company Accounting

Oversight Board (PCAOB) whose responsibilities include the quarterly review of certified financials from public companies. Another provision impacting records managers is a new seven year retention period for memoranda, correspondence, communications, other documents, and records (including electronic records), that are created, sent or received in connection with the audit or review and contain conclusions, opinions, analyses, or financial data related to the audit or review.



SOX creates criminal penalties including fines and up to 20 years in jail for altering, destroying, mutilating or concealing a record, document or other object with the intent to impair the object's integrity or availability for use in an official proceeding or for otherwise obstructing, influencing or impeding any official proceeding or attempting to do so. In addition, a failure to abide by minimum retention requirements can result in fines and up to 10 years in jail. These penalties have already been used. A June, 2004 article in CFO.com reports "In March the SEC fined Banc of America Securities \$10 million for stalling on providing evidence in an investigation: the company had claimed it would take too much effort to produce the required archived Emails. In December 2002, the commission fined Wall Street brokerage firms Deutsche Bank Securities, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp Piper Jaffray more than \$8million for failing to retain E-mails for the proper SEC-mandated retention period." Clearly SOX provisions, like other SEC information management provisions that predated them, (e.g.,

Proctor and Gamble was fined \$10,000 in 1998 for failing to retain e-mail to the disposition date required by statute,) mean business and will be enforced.

Electronic records such as correspondence, contracts, CAD drawings, etc., that are born digital and remain digital through their retention period, can be categorized in records series that govern their paper or film-based counterparts. While this may call for the alteration of file structures and close cooperation with the IT department, the method of information organization will be intuitive to a records manager currently administering records in other media; however, there are other types of electronic records that are not so simple to administer.

E-mail

One of the trickiest areas of electronic records management is e-mail. Some records managers suffer confusion when they consider e-mail a records series of its own. E-mail is NOT a records series (like accounts payable records) rather it is a communication channel (like snail mail or a telephone) which yields a record (like a paper letter or contract or an audio recording). A 2003 study by the ePolicy Institute, American Management Association and Clearswift of 1,100 U.S. companies showed that 14% of respondents had been ordered by a court or regulatory body to produce employee e-mail. A subsequent 2004 study by ePolicy and the AMA indicated that while 79 percent of companies surveyed reported having an e-mail policy, only half trained employees regarding the policy. As with other records and information management policy implementation, employees can only comply when they understand the policy and how to comply. For employees, or companies, adopting a "keep everything" or a "delete everything" policy, carry a box of snail mail into a staff meeting and dump it on the table in order to demonstrate how the subject matter of the e-mail should determine its value as a record.

Instant Messaging

Another serious electronic records challenge is Instant Messaging. This type of real-time chat client has grown to very wide use and , while the SEC has not directly addressed retention related to IM, companies are already preparing as though retention were required. In 2001, more than 100 million people were using Instant Messenger. By 2003, it was reported that more than 90 percent of companies have Instant Messenger users (sometimes without the cooperation of IT). In most cases, the IM client was a consumer-type client. So, within a single company, there could be three or more IM clients (though AOL Instant Messenger is the most common). Some companies are implementing commercial IM solutions, such as Lotus Sametime™. Software developers are also introducing hosted IM solutions which provide automatic capture. In the short-term, electronic records policies should recognize the need to capture and retain transcripts of IM sessions where business-related communication has taken place.

Conclusion

Many companies are now reacting with fear to records issues raised in Sarbanes Oxley. Like HIPAA and Gramm Leach Bliley, there are some vendors who will seek to take advantage of this climate. In a March, 2004 article in Transform magazine, author Bruce Silver states "SOX today provides the ideal vehicle for justifying the purchase of virtually any type of enterprise software. And that is what we have witnessed. Each vendor narrowly frames the SOX challenge in terms of its particular software capabilities, but in many cases those are tangential to the real problem. Despite the blizzard of webinars, white papers and magazine stories to the contrary, SOX compliance is not fundamentally a problem of records management. Yes, the Act specifically requires documents to be retained, but so does the IRS in the case of income tax records, and no one would suggest that tax preparation is at heart a records management problem."

THE TEN COMMANDMENTS OF ELECTRONIC RECORDS

- Let thy management support thy electronic records initiatives—for it shall go hard with thee if thy CEO should blindside thy program implementation.
- Know thy hardware and software, that the versions thereof may be migrated and thy legacy systems might be maintained if needs be.
- Remember thy data backup tapes, that thy retention and destruction schedules and policies should include them in their fullness, thereof.
- Thine employees shall knowest the technology use and security protocols, and shall abide by them, even unto the ends of their employment.
- Consider electronic records in thy policy statements, since thou knowest a record is a record, regardless of thy media type.
- Thou shalt establish for thy data every means of coming in and going forth, that protection shall be granted for thy importing and exporting and the fullness thereof.
- Thou shalt teach thy employees the electronic records policy.
- Thou shalt gird thy organization with a litigation response team, so that litigation shall not vex thee, nor electronic discovery make thee weary.
- Beware the remembrances of thy keystrokes and spirits in thy data; be thou mindful that when thou delete files, they shall not disappear until overwritten.
- Thou shalt not shred or destroy thy scheduled records, even thy scheduled electronic records and backup tapes, when a lawsuit doth press hard upon thee.

HIPAA, Gramm Leach Bliley and Destruction

Two industries which have received increased scrutiny regarding confidential destruction of sensitive documents are healthcare and financial services. This is due to the passage of two comprehensive pieces of legislation called HIPAA and Gramm Leach Bliley. The intent of both laws, and rules promulgated after the passage of those laws is very similar:

Information that is private or sensitive in nature must be safeguarded from unauthorized access. In addition to safeguards that protect this information while it is being used, there are also requirements that this information – once no longer needed – is disposed of in a way that maintains its confidentiality and security.

There can also be overlap between HIPAA and GLB. The organization Privacy Rights makes this observation about medical information in financial institutions. “The GLB covers information in the files of financial companies. You may not think your bank would have medical information about you in its files. But, it certainly could – if it were to receive information from its affiliated health insurance company, for example, or were to take note of your checks or credit card payments to medical facilities. Unfortunately, GLB does not give consumers any special protection for medical information.” Of course, depending upon the nature of the medical information, it may receive some protections under HIPAA.

HIPAA Overview

In the health care industry, there has been much confusion as to what is and is not required under HIPAA (Health Insurance Portability and Accountability Act) and its Privacy and Security Rules. Regarding destruction, HIPAA does not mandate a specific method of destruction; rather it infers a method by demanding that covered entities assess the potential for information

disclosures and create policies to prevent such disclosures. The types of information generally judged to be sensitive include protected health information (patient based information), regulatory review and incident report information, peer review and quality management documents and employment documents. In addition, business or transactional information such as billing information which may contain social security numbers, credit card numbers, personal financial data or Medicare identifiers are also considered sensitive. There are also other types of information generated including business information documenting internal business practices of the covered entity, etc., that may require careful handling because of its sensitive nature.

HIPAA creates a secure and private environment for Protected Health Information (PHI). Where interaction with confidential destruction companies is concerned, it also creates a relationship and a series of expectations between the "covered entity" (the records or information owner) and a "business associate" (confidential destruction vendor). This relationship is expressed in a contract or addendum containing a "Business Associate Agreement". Under HIPAA, this agreement must contain the following language: 1) Not use or disclose PHI in a manner that would violate any state, federal, or local law, including the HIPAA guidelines; 2) Ensure that there are appropriate safeguards to prevent use or disclosure of the PHI; 3) Immediately inform the facility of any use or disclosure of the PHI; 4) Ensure that any subcontractors and employees are aware of restrictions regarding the use or disclose PHI; 5) If required, make the PHI available to the appropriate parties in accordance with the HIPPA Guidelines; and 6) Make available for review any internal records regarding the management of PHI.

Gramm Leach Bliley Overview

Likewise, financial services companies have significant responsibilities under GLB. The final rule mandates "administrative, technical and physical safeguards: to insure the security and confidentiality of customer records and

information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." Indeed, even before the passage of GLB in 1999, financial institutions were frequently the targets of "dumpster diving" carried out by television camera crews who extracted mortgage applications, credit reports and other embarrassing items from the public solid waste stream. Also like HIPAA, GLB's directives are somewhat short on detail.

Specifically, 16 CFR 314.4 (b) of the final rule requires financial institutions and others managing consumer financial information to "Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations..." Clearly the proper disposal of information containing consumer information is central to preventing identity theft and other crimes. Shredding is a very effective method of maintaining the security of consumer information.

Information Disposal Considerations

Organizations governed by the privacy and security aspects of both HIPAA and GLB corporations have gone to extraordinary lengths to place information in an inaccessible area. Hospital switchboards are now unable to provide any information to visitors inquiring as to the status of a patient, and financial institutions have instituted heavy layers of encryption in order to shield electronic information from unauthorized access. It would stand to reason that secure disposal of information would also enter into the thinking of responsible persons. Unfortunately, this is not the case in some institutions.

Providing adequate physical safeguards to prevent the unauthorized access of information extends beyond the usable life of information. Security is no less necessary during the destruction process than when records are in use. And, should information fall into the hands of unauthorized persons during the destruction phase, the ramifications are potentially just as damaging.

When evaluating the capabilities and safeguards offered by records destruction vendors, there are many criteria for your consideration. The physical security barriers at facilities and on vehicles are a significant consideration. Equally important are the screening processes for employees, challenge and verification procedures for individuals wishing to witness destruction at an offsite facility, and after-market use of shredded materials. The National Association for Information Destruction provides a certification program for information destruction companies. For more information browse to www.naidonline.org.

Initial Assessment

In order to understand the complete risk of exposure, it is necessary to understand where information may be inadvertently disclosed. The most obvious starting point is to assess each department to determine what type of information output is generated, and which types of information generated require confidential and secure protection and disposal. In addition to interviewing employees and observing work methods and processes, a trip to the dumpster is also in order.

A waste assessment is a quick way to discover how much sensitive information is finding its way into unprotected areas of the organization. Additionally, this assessment will also demonstrate which departments may need to receive supplementary training, remedial education, or enhanced equipment. Your offsite confidential destruction vendor can be very helpful to you in conducting this audit process and in determining the placement of secure receptacles to receive confidential information.

Following the assessment, additional training and remedial education regarding secure and non-secure documents, many organizations find it helpful to station locking bins or consoles in various departments to encourage the proper disposal of confidential information. Most will coordinate this placement with their vendor in order to select the proper size and capacity. Just as an audit method was used to insure compliance with confidential disposal methods – you can also work with your vendor to make sure only confidential information is finding its way into destruction bins. Spot checking trash receptacles and destruction bins on a periodic basis is a great way to insure compliance with information protection programs.

Chain of Custody Issues

The purpose of using an outside vendor is to provide a secure information destruction solution. Establishing a precise chain of custody of secure information is central to minimizing the risk of inadvertent exposure. As long as information is at the health care or financial services facility, employees of that facility are responsible for keeping the information secure. When information is transferred to a confidential destruction vendor, the responsibility for securing this information becomes the vendors. The information protection plans should incorporate this chain of custody into the overall destruction process by seeking answers to such questions as “How is information protected while in transit to the destruction facility?”; “How long is information retained before being destroyed?”, and “How is information protected at the destruction facility prior to being destroyed?” By reviewing the procedures of your confidential destruction vendor, you will be able to document a chain of custody and types of protection in place throughout the life of the information. All shredded materials are destined for re-use in some form. Some may be re-pulped to become office paper or other household products like facial tissue. Other shredded material may be used for animal bedding or mulch. The fact that shredded materials are recycled in some form means that the method is more environmentally friendly than incineration. Some organizations

may feel that the simple act of recycling without shredding is sufficient for the protection of sensitive information. Nothing could be further from the truth. Even when recycled materials are baled, information is still completely accessible and readable. Additionally, baled materials may not be in a secured environment in transit to the paper mill. This presents opportunities for information items to break loose from the bale. If information is confidential in nature, or is mandated for protection, as in the case of HIPAA and GLB, information should be rendered unreadable as soon as the materials are no longer needed.

Witnessed Destruction

If information is particularly sensitive, or if an information protection procedure has been established to require it, some organizations wish to have an employee witness the destruction of confidential materials. This is accomplished in three ways: 1) bringing a mobile shredding vehicle to your facility; 2) sending an employee to the destruction facility; or 3) watching the destruction via Internet link or video tape. Not all confidential destruction firms offer all three methods, so check with your vendor to determine which options are open to you.



Certificate of Destruction

While a significant portion of information for destruction might consist of daily or weekly non-record work output, there will occasionally be official record materials that require destruction. In order to effectively close the documentation loop, a certificate of destruction is placed on file when

these records materials are removed from inventory. This step is especially important for records managers because 1) It shows that records retention schedules are applied in the ordinary course of business and are not arbitrary; and 2) There is a documentary history of the inventory destroyed that can be

produced in evidence during the discovery phase of litigation. Proper adherence to the procedures described in this article will help you do your part to safeguard medical and financial information protected by HIPAA and Gramm Leach Bliley.

Business Records Management provides information management services to over 3,000 organizations throughout Pennsylvania, Ohio, Maryland, West Virginia, and parts of New York. BRM's services include Document Management and Delivery Services; Disaster Recovery Planning, Support and Facilities; Software Escrow; Certified Destruction Services; Computer Media Storage and Rotation; Records Management Consulting, and Electronic Vaulting (E-vaulting).

If you would like more information, please contact Business Records Management at 412-321-0600, or via email at brmdetails@businessrecords.com.