



THE INFORMATION MANAGEMENT DIGEST

Our Business, Is Keeping Your Business - Your Business!

A Service of WesTex Document, Inc.

May 2011

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 HIPAA 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 off-

site 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.



Cost of Corporate Data Breaches Rises

In 2009, the cost of a data breach was \$6.8 million; in 2010 the cost went up 5% to \$7.2 million. According to a NetworkWorld article, Ponemon Institute conducted its annual study of data loss costs last year and looked at 51 organizations from various industries who agreed to discuss the impact of losing anywhere between 4,000 to 105,000 customer records. The survey revealed that "negligence" was the main cause of data breaches in 2010, and "malicious or criminal attacks" were the most expensive type of data breach.

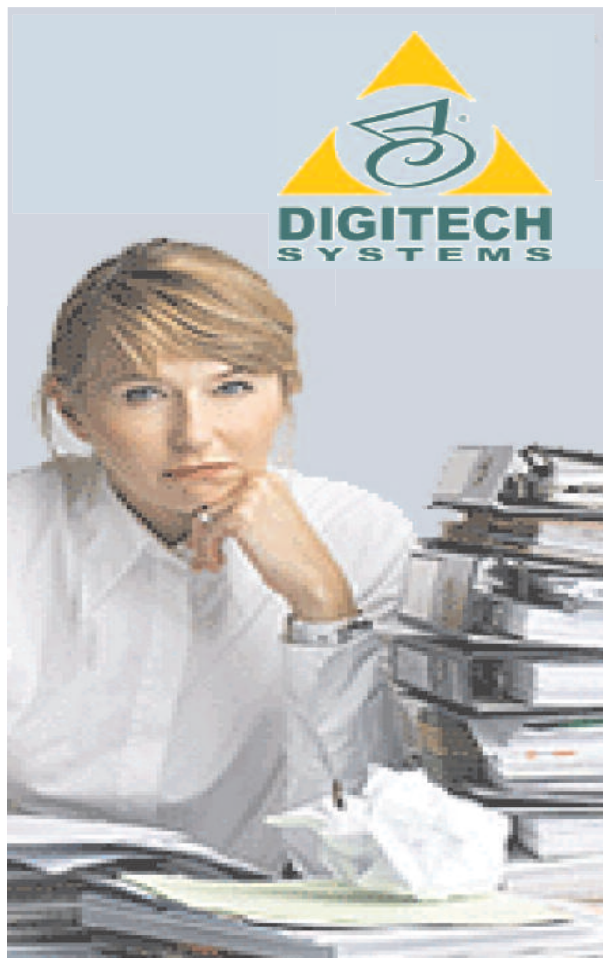
The article noted that last year there also were a few instances of data breaches that companies said were due to mistakes made by their cloud service providers. One financial service company suffered from a data breach because its records were exposed on a shared virtual machine server that others using the cloud-based service could see.

Although negligence accounted for 41% of data breach cases, for the first time, malicious or criminal attacks was reported in 31% of cases.

According to the article, malicious or criminal attacks are the most expensive type of data breach to discover and respond to because they are harder to detect. "It's harder to detect and do investigations," said chairman and founder of the Ponemon Institute, Larry Ponemon, Ph.D., about cases involving malware and botnets or social engineering. "Just two years ago, only 12% of data breaches were ascribed to malicious and criminal activity," he continued.

The Ponemon survey revealed that the average cost of a "malicious or criminal attack is \$318 per customer record, \$151 more than non-malicious breaches that stem from negligence or system failures. System failures were reported to be the third-leading cause of data breaches.

The article noted that Ponemon reported that the cost was higher for companies that moved quickly to notify victims of the breach. According to the article, some industries last year saw higher costs per customer record in a data breach than others, with upward spikes. The survey reported that financial services jumped to \$353 per customer record in 2010, up from \$249 in 2009, and healthcare jumped to \$345 last year from \$301 in 2009. The communications sector had the highest cost of all, at \$380 per customer record. Media, at \$131, education at \$112, and the public sector at \$81 stood at the lowest.



Wasting Time with Paper?

Then relax, there is a better electronic way.

Improve performance with instant file access.

Increase efficiency with automated workflow

"The labor savings were immediately apparent. We can index and input a couple thousand documents in just minutes."

Digital imaging, microfilm, storage and destruction.



WesTex Document, Inc.
Amarillo and Lubbock
www.westexdocument.com
(806) 885-2906

