



A service of BUSINESS RECORDS MANAGEMENT LLC

3rd Quarter 2010

## PLAYING BY THE NEW HIPAA RULES

Within the American Recovery and Reinvestment Act of 2009 (ARRA) that was signed into law on February 17, 2009 were changes for HIPAA (Health Insurance Portability and Accountability Act) to strengthen privacy and security for personal health information (PHI). The Health Information Technology for Economic and Clinical Health Act, called the HITECH Act, is the vehicle for changes that will significantly increase penalty amounts for violations of HIPAA rules covering PHI.

The HITECH Act has a wider purpose than preventing breaches of health information. An overview written by the Majority Staff of the committees on Energy and Commerce, Ways and Means, and Science and Technology (January 16, 2009) states that this act will advance the use of health information technology (Health IT) such as electronic health records by developing standards by 2010 that will make electronic exchange of information possible. It will invest \$20 billion in HIT infrastructure as well as offering incentives to physicians and hospitals who treat Medicare and Medicaid patients to use electronic patient health information. Its intent is to save the government \$10 billion by reducing duplicative care and medical errors while improving care coordination. And as the health care sector uses more Health IT, and produces more records with personally identifiable health information, the Act strengthens federal privacy and security laws and hands out stringent punishment for failures.



### What is a "Business Associate"?

The HIPAA Privacy Rule applies only to covered entities—health plans, health care clearing houses, and certain health care providers. However, there are many functions that are performed by external businesses or persons and these are known as "business associates." The covered entities can release protected information to these associates—if they have satisfactory assurances that the external associates will use the information only for the purposes set forth by the covered entities, and that it will be safeguarded in ways that will help the covered entities comply with HIPAA's Privacy Rule.

"Satisfactory assurances" that the protected health information received or created by a business associate will be safeguarded must be in writing as a contract or other agreement. (Go on line to 45 CFR 164.504(e) for details.)

The U. S. Department of Health and Human Services (HHS) states that business associate functions and activities can include data analysis, processing or administration as well as processing claims, quality assurance, billing and other functions. HHS views data aggregation as a service as well as legal, accounting, actuarial, administrative and other services.

There are transition provisions for existing contracts: see CFR 164.532(d) and (e), and there are exceptions to the standard for business associates: see 45 CFR 164.502(e). There are even situations in which a business associate contract is not required; see [www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates).

Storage companies which are members of PRISM have access to a Business Associate Agreement developed to adhere to HIPAA regulations. This is an excellent format for creating the contract you may need.

### **There are federal requirements for breach notifications.**

Within the HITECH Act, there are sections that establish a federal notification requirement when health information that is not encrypted or otherwise made indecipherable (referred to as unsecured) has been breached.

Section 13402, Notification In The Case of Breach, states that a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, upon discovering a breach, notify each individual whose unsecured information has been, or likely has been, breached. A business associate who maintains unsecured information as described must notify the covered entity with identification of each individual. All notifications must be made without delay, no later than 60 days after discovery of the breach. Written notice by first class mail must be sent to each individual or next of kin, or by email if the individual has chosen that communication method.

If there are 10 or more persons for whom there is out-of-date or insufficient contact information, a

conspicuous posting with a toll-free phone number must go up on the web home page of the covered entity. Or a notice must run in major print or broadcast media.

If the unsecured protected health information of 500 or more residents of a state or jurisdiction has been breached, notice is given to prominent media outlets serving that area. And a notice is sent to the Secretary of Health and Human Services who then puts a notice on the HHS website listing the covered entity(ies) involved.

The notification sent to individuals must include, to the extent possible, a description of what happened with date of breach and date of discovery; types of information involved such as full name, Social Security number, date of birth, home address, disability code, or account number. There must also be information as to

what a person can do to protect themselves from harm; what the covered entity is doing to rectify the situation; and a contact method so that persons can get additional information. The Secretary of HHS will prepare a yearly report on the number and nature of breaches reported, and response actions taken in each situation. Section 13407, Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities. A vendor of personal health

records who discovers a breach of security of unsecured PHR identifiable health information must notify each individual who is a citizen or resident of the United States and whose personal information was breached, and the vendor must also notify the Federal Trade Commission. A third party service provider who finds a breach in a vendor's information must notify that vendor or entity with identification for each individual affected. Procedures set forth in Section 13402 above are applied here as well, but this violation is treated as an unfair and deceptive act under FTC regulations.

### **Tougher penalties are part of the HITECH Act.**

Section 13410, Improved Enforcement. This revises Section 1176 of the Social Security Act



(42 U.S.C 1320d-5) to strengthen enforcement of HIPAA rules. Section 1176(a) establishes categories of violations which show increasing levels of culpability. It requires that a penalty be based on the nature and extent of the violation, and the nature and extent of the harm that resulted from the violation. It sets forth the tiers of increasing penalty amounts. These in turn establish the range of the Secretary of HHS's authority to impose civil money penalties.

### **Want to get more information on HIPAA?**

One source is [www.hipaasurvivalguide.com](http://www.hipaasurvivalguide.com) which offers free material ranging from a list of HIPAA General Administrative Requirements with relevant notes that explain in layman's language what each section means and how it will affect those responsible for safeguarding health information, to specific language on each section of the HITECH Act. Another source is [www.hhs.gov/ocr/privacy/hipaa](http://www.hhs.gov/ocr/privacy/hipaa) with pages of information on health information privacy. As a business associate responsible for the security of records, your storage contractor has a stake in complying with the HITECH Act and can provide information.

## **BEING A RECORDS DETECTIVE: WHEN EMPLOYEES LEAVE, ARE RECORDS LEAVING TOO?**

Apparently ethics have evaporated into the Ethernet. A survey to determine what is happening with electronic data used by employees who leave for another job or are terminated revealed that 59% of these employees had stolen proprietary data. Furthermore, 79% of these employees knew that their employers did not permit such movement of company data.

Asked how they would use this purloined information, 67% said they used it to leverage a new job. This is risky business, according to Gavin Manes of Avansic, a digital forensics company. Persons who provide confidential information to a new employer or competitor can bring legal action down upon themselves, upon their potential employer, and upon their past employer if stealing produces a privacy breach of personal information.

These findings came from a study titled Data Loss Risks During Downsizing which was sponsored by Symantec and conducted by the Ponemon Institute ([www.ponemon.org](http://www.ponemon.org)), with results revealed in February 2009. Survey respondents were 945 adults in the USA who had been fired or laid off or who had changed jobs in the previous 12 months. All had use of laptops or a desktop computer with access to proprietary, sensitive or confidential information. (One view of this survey is that since it was web based, the exemployees may have sought out this survey in order to participate. This could skew the figures higher than if the survey had been a truly random survey of such persons.)

The survey's intent was to see to what extent exemployees took data with them, and to ask how they justified such actions. Moreover, the survey sought to determine the types of information that are most susceptible to theft, and to identify how companies can protect themselves from losing valuable data.



### **How do they get away with it?**

Ex-employees steal information by taking paper documents or hard files (61%). Or by downloading data onto a CD or DVD (53%) or onto a USB memory stick (42%). Some send documents as an attachment to their personal email account (8%).

What do they take with them? Email lists (65%), nonfinancial business information (45%),

customer contact lists (39%), employee records (35%), and financial information (16%).

What are companies doing to prevent data theft? Not much, according to the ex-employees. After leaving, they still had access to company data (24%) and that continued for a week or longer for 35% of them. Even when departing employees (4%) told their employers they were taking data, only 15% of these companies reviewed or audited the data being taken.

So *why* do they get away with it?

Because “more and more people seem to feel entitled to information they create on the job...as more employees work from remote locations and on home computers, the concept of who really controls this data isn’t often clear to people,” according to Larry Ponemon.

Too many companies are lax about cutting off access to systems for ex-employees. A survey funded by Symark International, Inc. ([www.symark.com](http://www.symark.com)) learned from 850-plus respondents that 27% had more than 20 orphaned accounts still active, and 42% admitted they did not know how many orphaned accounts they had nor if they were still being used. Asked how many exworkers still had live accounts, 8% said their companies had 100 or more.

Ideally a company should have a policy for forensic storage in its employee manual along with statements on computer usage and access. This gives a heads-up to employees that the employer will aggressively protect company data including trade secrets and intellectual property.

How to do this is spelled out by Jason Park in an article titled “Defensive Exit Interviews and Records Retention for Departing Employees” ([www.lsilegal.com/misc/ELS.htm](http://www.lsilegal.com/misc/ELS.htm)). For example, when an employee leaves and his/her computer and storage devices are turned in, a forensic copy of their hard drive should be made immediately before the devices are reformatted for use by another employee. This copy can be used if necessary to prosecute theft of intellectual property. When all employees know that this is standard procedure, it can act as a deterrent to data theft. Using licensed or certified persons to make these forensic copies should safeguard the integrity of the original electronic file. Two copies should be made: one to be the forensic “pristine” copy, the second to be the “working” copy.

## **So, what would look like suspicious activity?**

Viewing the working copy, look for such things as very large file transfers or unusual files residing locally, like a customer list. Also types of files that the employee would not normally use, or large files with recent date stamps. Watch for use of files at odd times such as after hours, weekends or holidays. Be alert to more outbound e-mails than in the past and changes in software—added, deleted, upgraded or downgraded.

One company providing these forensic services is eMag Solutions ([www.emaglink.com](http://www.emaglink.com)) with its Departing Employee Data Capture program which claims to find files that have been hidden through renaming, password protection, encryption or compression. If all of this seems like a lot of work, be aware that it is estimated that the theft of intellectual property costs U. S. businesses \$59 billion dollars a year.

## **How to put some emphasis into the exit interview.**

If the departing employee signed an employment agreement saying that the employee would maintain in confidence trade secrets of the organization, or trade secrets created by that employee during his/her time of employment, then the exit interview provides an opportunity to review and reinforce these obligations and how they will affect the employee’s conduct after leaving the company. This is certainly the case if the original employment document contained a non compete clause spelling out the length of time in which the departing employee can not work for a competitor nor start a competing business.

Trade secrets should not be used for the benefit of a future employer. If this happens, a former employer may bring suit not only against the former employee, but also against the new employer as well. In April 2009 Starwood Hotels and Resorts Worldwide, Inc. filed suit against Hilton Hotels Corporation and two senior Hilton executives. The executives had formerly worked for Starwood and were accused of stealing more than 100,000 electronic files of proprietary and confidential Starwood information.

Both the employee and the employer should have copies of the signed employment agreement, and both should have copies of the

exit interview results. This is useful because over time there can be changes in those who handle employee records and in document retention policies. Arnold B. Silverman writes frequently about the legal aspects of employment matters. Look for "Employee Exit Interviews—An Important But Frequently Overlooked Procedure" at [www.JOM.53\(11\)\(2001\), p. 48](http://www.JOM.53(11)(2001), p. 48).

From a records management point of view, the protocol established by the University of Greenwich for exiting staff puts responsibility on the departing person to systematically identify and organize the records he/she is responsible for. Using this list as an overview, the organization's records manager could determine what information the departing employee has been using, and could look for irregularities in usage. ([www.gre.ac.uk](http://www.gre.ac.uk), search for records management.)

To get assistance in formulating a data security plan that extends to exiting employees, talk with your storage contractor.

## **DIGITAL COPIERS PROVIDE UNINTENDED PORTAL FOR IDENTITY THEFT**

At the moment your company trades in its old copier, you may have just released 10-15,000 pages of sensitive documents to the next owner of the machine. CBS news and other news outlets have created a firestorm of public concern after airing stories identifying digital office copiers as a major source of potential identity theft.

Articles highlighting the risks inherent in trading in copiers have evidently been known for some time by copier companies, but are only now making their way into mainstream news. In reporting their story, CBS spoke with the President of Sharp Imaging, a digital copier company, who was asked whether the industry had failed to adequately warn consumers and businesses about the dangers of digital copiers. "Yes," was his response.

"It's falling on deaf ears," McLaughlin said. "Or people don't feel it's important, or 'we'll take care of it later.'"

Even though the copier industry may not have been successful in getting the word out, according to McLaughlin there have been substantial efforts to spread the word. CBS news reported that Sharp commissioned a survey in 2008 that found that 60% of Americans were completely unaware that digital copiers stored images on their hard drive. They are, in fact computers – a fact noted by Toronto computer science professor Graeme Hirst as reported on the blog Rich's Random Walks.

"Modern, large, office-type photocopiers are computers. The whole system is controlled by a computer, it has a hard disk. It scans images and they are stored on the disc," said Hirst. "They are also networked computers, and they have all the same security issues that a computer does, so all the same security issues arise," he said. The article concludes by noting "It really makes no sense to have a strict security policy for your office computers, if the photocopier is down the hall passing out information to anyone who asks. These machines, like PBX equipment, need to be secured with the same care that the computers get."

Even though office machines may not fall in the records management department or under the control of information management, a complete review of the information system of the organization should include any digital office machine which is capable of storing information. Some issues of compliance with HIPAA, Sarbanes Oxley, Red Flag Rules or FACTA, are sure to require the inclusion of digital copy machines in any audit or system review.

## **LIVING IN THE AFTERMATH OF NEW TECHNOLOGY IMPLEMENTATION**

As the 60s-era television commercial used to say, "We've come a long way, baby". From cave drawings to stone-carved hieroglyphics to scrolls, printed books, spindled originals, metal filing cabinets bursting with birth and death certificates in basements of courthouses and microfiche-filled research libraries – media is well on its way to existing in an exclusively digital format. Despite the range of technical innovations, the question remains: is the job of a

records and information manager easier or harder thanks to this technology.



### **Drowning in Data or Sailing On the Next Wave?**

Peter Drucker coined the term “knowledge worker” three decades before the existence of the Internet. In describing this type of worker he anticipates the fierce pace of change in his third factor of knowledge worker productivity, “Continuing innovation has to be part of the work, the task and the responsibility of knowledge workers.” Even though there have been disruptions to some aspects of the population, (ask someone working in a US textile factory if you can find one), the transition from the industrial to information age has brought many benefits to individuals – records managers being no exception. For good reason then, more jobs are being created in the knowledge sector than in any other. According to the authors of *Management Information Systems for the Information Age*, “Knowledge Workers are now estimated to outnumber all other workers in North America by at least a four to one margin.”

But are these knowledge workers more productive? It depends on whom you ask. In his blog *Workplace911*, Robert Bacall believes that technology and productivity are not necessarily related. “We just aren't very good at squeezing

out the productivity enhancement potential that is inherent in technology. Technology, in itself, is not sufficient to produce improvement.” William Reader, professor of psychology at Sheffield Hallam University, disagrees by pointing up at least one positive aspect of technology saying “As our social networks are becoming increasingly more geographically fragmented, social network sites are a useful way for us to keep in touch and seek social contact with our friends.”

Regardless of whether we agree with the impact of technology on our lives, we must deal with it effectively. Even disciplines long known for the permanent preservation of paper records, the National Archives and Records Administration (NARA), has invested heavily in its Electronic Records Archives, an effort to create a “permanent” solution to the constant challenge of preserving electronic records. With input of industry leaders, the federal agency is attempting to establish a dynamic system to store and access records. “There has been a race against technology as we watch software become obsolete almost as soon as it is installed in our computers,” said former Archivist of the United States Allen Weinstein. “All of us have stored personal memories or favorite music on eight track tapes, floppy disks, or eight mm film. In many cases, these technologies are now relics and we have no way to access the stored information. Imagine this problem multiplied millions and millions of times—that’s what the federal government is facing today. But thanks to ERA, the technology for preserving electronic records is finally beginning to catch up with the technology for creating them. This Initial Operating Capability is a crucial step in ensuring that our recent history will be saved.” And how much information are we talking about? To put this scope into perspective, researchers at University of California, San Diego, (in their study titled “How Much Information”), determined that American households collectively consumed 3.6 zettabytes of information in 2008. One zettabyte equals one billion trillion bytes, the number formed by a one followed by 21 zeros. The report suggested that a single American consumes 34 gigabytes of content and 100,000 words a day of various media, including books, television, the Web, movies, text messages and video games, among others. And the proportion of digital information continues to grow. According to

magnetic or optical media and 20% on fixed media. The book *Storage New Horizons* notes that 92 percent of newly created data is digitally based and that eight percent has an analog origin of paper, film or other media.

### **Separating the Help from the Hype**

Clifford Stoll, in his book *Silicon Snake Oil*, seems particularly fed up with the unfulfilled promises of cyberspace. "'Few aspects of daily life require computers... They're irrelevant to cooking, driving, visiting, negotiating, eating, hiking, dancing, speaking, and gossiping.'" Most people would agree that you don't need one to write a book like *Silicon Snake Oil* either, but they do save a lot of time and speed up the editing process. That being said, Stoll raises an interesting point about the complete interdependence of human beings on guiding whichever flavor of technology is selected. The records management listserv carried the following posting on this subject.

"As far as the longevity issue goes, in my humble opinion, the most important factors in so-called "digital preservation" are NOT the technology factors (tricky as they are), but rather the human and the institutional and social factors," noted Fred Grevin, Deputy Commissioner and Chief Information Officer for the City of New York. "Humans, human institutions and human societies are really terrible at actively-preserving things, and active preservation is what would be required to successfully-preserve computer data." "It should be clear by now that merely selecting high-quality computer data storage media and putting them on a shelf is not a viable approach to the preservation of computer data for the long term (anything greater than the traditional definition of a human generation, 25 years)," added Grevin. Paper records, sometimes referred to as "training edge technology", are likely to remain an integral medium for records management for the foreseeable future, if for no other reason than to provide a stable alternative to intermediate records storage until some types of digital preservation can be proven effective and resilient. The shift of digital working copies seems very far along and probably represents the arrival of the "less paper office" as a reality.

### **Managing the human touch**

In many respects the same difficulties that have plagued records and information management continues to impact the discipline. The application of policies, (or lack of effective policies related to information management,)

has created high profile problems regardless of the technology involved. The Apollo 11 slow-scan television tapes that captured Neil Armstrong and Buzz Aldrin's first lunar footsteps, represented primary source material that was forever lost because NASA policies directed that the medium be reused. The original broadcast of the July 21, 1969 moonwalk was transmitted using the highest quality recording technology of the time.

Today's viewers are limited to grainy sights and scratchy sounds because the images are essentially copies of inferior video conversions of the historic moment. Did this represent a mistake on the part of a NASA employee? No. The employee was following a policy made necessary by the fact that the tapes were no longer being manufactured. The policy did not contemplate the need to make an exception for the historic nature of the Apollo 11 landing.

So, is it easier to be a records manager in a world awash in technology? Probably not. There are more hazards and difficulties than ever before. Fortunately technology also brings with it new opportunities to drive business value and elevate the organizational value of the information management professional. As for life in the midst of technology, Eric Bautista, an Eighth Grader from Silicon Valley was interviewed by ABC News about technology and summed it up this way "It's bad for us, but it sure is fun."

## **ARMA INTERNATIONAL TESTIFIES ON "FEDERAL ELECTRONIC RECORDS MANAGEMENT"**

ARMA International was invited to provide testimony on "Federal Electronic Records Management: A Status Report" to the U.S. House of Representatives' Information Policy, Census, and National Archives Subcommittee on June 17, 2010. The panelists reviewed the status of management of electronic records at federal agencies, and explored ways to improve the scheduling and preservation of electronic records.

Carol Brock, CRM, represented ARMA International regarding the management of electronic records in federal government agencies during the hearing. Based on her extensive knowledge

of federal electronic records, Brock, who has been an ARMA International member for more than 23 years, testified to the challenges agencies face in scheduling and preserving electronic records. Additionally, Brock suggested a position of "Chief Records Officer" for each agency as a way of increasing recordkeeping reliability. She also addressed the role of the National Archives and Records Administration (NARA) in oversight of federal records.

At the hearing, ARMA International reinforced the concept of GARP® as a solution to federal agency records management challenges. During her testimony, Brock recommended, on behalf of ARMA International, that GARP®'s bedrock records management principles should be integrated into the operation of every federal agency. ARMA International members Dr. Gregory S. Hunter, CRM, and Paul Wester also testified to the congressional subcommittee – although not as representatives of the association. Hunter has been a member since 2005 and is an associate professor of library and information science at Long Island University. Wester joined ARMA International in 2004 and is the director of the modern records program for NARA.

## **ARMA INTERNATIONAL INTRODUCES NEW RESOURCE FOR INFORMATION MANAGEMENT**

This book is a must-have resource for anyone new to managing information within an organization, or for those individuals who are trying to simplify the process of records retention. Helping your organization toward better business practices – being more efficient, more competitive, and more compliant – starts here. Every organization has records in many different forms with different requirements and lifecycles. This often raises questions about what to keep, for how long, and how to establish that process. The answer to these questions – and to having a successful recordkeeping program – is a records retention schedule.

Often the responsibility of managing an organization's information falls to an individual or group of individuals who have no background with information management. For them, creating a retention schedule becomes one

of the first and most important things to establish. In John Montaña's new book *How to Develop a Retention Schedule* he explains, in a clear and straight forward format, what a records retention schedule is, the process for creating one, and why they are necessary for proper records management.

This great new resource clarifies procedures for data collection, drafting, structuring, and developing retention periods. Its chapters focus on indexing, legal research, strategic considerations, litigation, and more, which gives readers the information necessary to create a working retention schedule and offers tips for keeping it updated.

"The number one question we get from people is 'How do I develop a retention schedule,'" says Marilyn Bier, Executive Director for ARMA International. "This book is a must-have resource for anyone new to managing information within an organization, or for those individuals who are trying to simplify the process of records retention. Helping your organization toward better business practices – being more efficient, more competitive, and more compliant – starts here."

Find *How to Develop a Retention Schedule* and other information management resources at [www.arma.org/bookstore](http://www.arma.org/bookstore). Interested in reviewing this book? Contact Ashley Flynn at [ashley.flynn@armaintl.org](mailto:ashley.flynn@armaintl.org).