
INDUSTRY NEWS

AUGUSTA DATA STORAGE

A Service of Augusta Data Storage, Inc.

1st 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 clearinghouses, 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.

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 above 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 e-mail 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 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 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.

ARMA International Releases Three New Guidelines for Information Management

Standards, guidelines, and technical reports are designed to create a professional best practice environment within an organization. ARMA International continuously releases new and up-to-date guidelines to keep information management professionals current on these best practices in growing industries, professions, and technologies.

(Vocus/PRWEB) November 25, 2009 -- Standards, guidelines, and technical reports are designed to create a professional best practice environment within an organization. ARMA International continuously releases new and up-to-date guidelines to keep information management professionals current on these best practices in growing industries, professions, and technologies. Following are the latest additions to the ARMA International Standards and Best Practices family:

Website Records Management Guideline:

This guideline explores how information posted on websites may constitute records. It offers records and information management (RIM) advice and best practices recommendations for managing website records. It covers roles, responsibilities, and risk management for website management, including website lifecycle issues, technologies for creating and attaching metadata, web content management, capturing and harvesting website data, and meeting the challenges of Web 2.0.

RIM for IT Professionals Guideline:

Electronic commerce, emerging technologies, privacy and security requirements, and other business drivers are requiring RIM and IT professionals to join forces. This guideline is designed to help RIM professionals extend their IT knowledge while assisting IT professionals in gaining a clear understanding of records retention and archiving requirements and methodologies. It provides guidance for professional collaboration between records managers and IT to create cohesive information management solutions.

Contracted Destruction for Records and Information Media:

Designed to guide organizations when contracting for destruction services, this guideline identifies the critical components that must be addressed so no records or information in any format are compromised during any part of the destruction process. For service providers, this guideline will create an understanding of the requirements for managing and processing an organization's records and information media destruction activities.

HHS Promises \$80 Million to Support Health IT Workforce

David Blumenthal, M.D., the U.S. Department of Health and Human Services' (HHS) national coordinator for health information technology, announced plans to make available \$80 million in grants to help develop and strengthen the health information technology workforce. The grants include \$70 million for community college training programs and \$10 million to develop educational materials to support these programs. Both programs will support the immediate need for skilled health information technology (health IT) professionals who will enable the broad adoption and use of health IT throughout the United States.

Authorized by the American Recovery and Reinvestment Act (ARRA), the grants are the first in a series of programs to help strengthen and support the health IT workforce. Additional details regarding the grant programs for these and other key resource and training areas will be announced in the near future.

"Ensuring the adoption of electronic health records (EHRs), information exchange among health care providers and public health authorities, and redesign of workflows within health care settings all depend on having a qualified pool of workers," said Blumenthal. "The expansion of a highly skilled workforce developed through these programs will help health care providers and hospitals implement and maintain EHRs and use them to strengthen delivery of care."

The community college program will establish intensive, non-degree training that can be completed in six months or less by individuals with some background in either healthcare or IT fields. Participating colleges will coordinate their efforts through five regional consortia that span the nation. Graduates of this training will fill a variety of roles that assist healthcare practices during the critical process of deploying IT systems and support these practices on an ongoing basis.

The curriculum development program will make high quality educational materials available to the community colleges so these training programs can be established quickly to meet the workforce needs.

Any U.S. non-profit institution of higher learning currently engaged in providing training in health IT that is interested in drafting curriculum or establishing a consortium that includes community colleges may apply for the grants. Information about grant applications will be available soon at <http://healthIT.HHS.gov/HITECHgrants>.

House Passes Data Breach Bill

On December 8, the U.S. House of Representatives passed the Data Accountability and Trust Act (H.R. 2221) via voice vote. The measure has been sent to the Senate for consideration.

Sponsored by Rep. Bobby Rush (D-IL), the legislation:

- Requires the Federal Trade Commission (FTC) to promulgate regulations requiring each person engaged in interstate commerce that owns or possesses electronic data containing personal information to establish security policies and procedure
- Authorizes the FTC to require a standard method or methods for destroying obsolete, non-electronic data
- Requires information brokers to submit their security policies to the FTC in conjunction with a security breach notification or on FTC request
- Requires the FTC to conduct or require an audit of security practices when information brokers are required to provide notification of such a breach.

Further, the bill requires information brokers to:

- Establish procedures to verify the accuracy of information that identifies individuals
- Provide to individuals whose personal information it maintains a means to review that information
- Place notice on the Internet instructing individuals how to request access to such information
- Correct inaccurate information

The measure directs the FTC to require information brokers to establish measures that facilitate auditing or retracing access to, or transmissions of, electronic data containing personal information and prohibits information brokers from obtaining or disclosing personal information by false pretenses (also known as "pretexting").

On the House floor, Rush stated the following about the legislation:

"Bill H.R. 2221 addresses data breaches by requiring 'for-profit' entities holding data containing people's personal information to have reasonable and appropriate security measures in place to protect that data. H.R. 2221 would also require them to notify consumers, who are U.S. citizens or residents, and the Federal Trade Commission when a breach occurs.

For the past five years, the Privacy Rights Clearinghouse contends that nearly 340 million records 'containing sensitive personal information' have been 'involved in security

breaches. High-profile data breaches have plagued financial institutions, nationwide retailers, online merchants, information brokers, credit card processors, health care institutions, high-tech companies, research facilities and government agencies.

"Currently, several laws address data security requirements for narrow categories of information or specific sectors of the marketplace. These laws include the Gramm-Leach-Bliley Act ("GLB Act") Safeguards Rule, which contains data security requirements for financial institutions, and the Fair Credit Reporting Act ("FCRA") Disposal Rule, which imposes safe disposal obligations on entities that maintain consumer report information. In addition, the FTC has used its enforcement authority under the FTC Act to bring actions against companies that have made misleading claims about data security procedures or who failed to employ reasonable security measures in circumstances causing substantial injury. However, there is no comprehensive federal law that requires all companies that hold consumers' personal information to implement reasonable measures to protect that data. Also, there is no federal law that requires companies that experience a data breach to provide notice to those consumers whose personal information was compromised. Those entities, who determine that there is no reasonable risk of identity theft, fraud, or other unlawful conduct, would be exempt from providing nationwide notice to affected persons under H.R. 2221.

"The DATA Act establishes a rebuttable presumption in the law that encryption-based technologies and methodologies adequately meet the determination standard in Section 3, subsection (f)(2)(A) of the Bill. More narrow exemptions are provided for a defined category of personal information holders known as "service providers," in addition to information brokers who handle protected data, but only for the limited purposes of preventing fraud. In promulgating the regulations under this subsection, the FTC may determine to be in compliance any person who is required under any other Federal law to maintain standards and safeguards for information security and protection of personal information that provide equal, or greater, protection than H.R. 2221."

The legislation passed with bipartisan support. The Senate is considering a similar measure, the Personal Data Privacy and Security Act of 2009 (S. 1490).



Augusta Data Storage, Inc.
3122 Mike Padgett Hwy.
Augusta, GA 30906
706-793-0186
888.299.0186