



**BUSINESS RECORDS MANAGEMENT**  
*Your Peace of Mind is Our Priority*

## ***ARRA: The Biggest Development in Healthcare Security Since HIPAA***



*a BRM White paper | Published November 2009*

The American Recovery and Revitalization Act of 2009 (ARRA) was approved by Congress on February 13, 2009 and signed into law by President Barack Obama on February 17, 2009. The Health Information Technology for Economic and Clinical Health (HITECH) Act provisions of ARRA include important changes in privacy and security to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Many of these changes will require businesses to change the way they currently do business.

In what ARRA describes as “improvements” to existing law, the healthcare industry will be subject to more rigorous standards regarding protected health information (PHI). Several well-publicized PHI breaches in recent years and the general lack of enforcement contributed to these changes.

Previously, HIPAA applied only to Covered Entities regarding the use and disclosure of PHI. Covered Entities are collectively defined under HIPAA as healthcare providers, healthcare clearinghouses and health plans. The new provisions affect not only Covered Entities, but a wide range of vendors and contractors that provide services to healthcare organizations.

Under ARRA, Covered Entities now include web-based companies that collect Personal Health Records (PHR). When HIPAA was passed, the Internet and online healthcare services were in their infancy. Now, a wealth of information relating to the past, present and future payment relating to an individual’s condition resides somewhere online. Under the new law, HIPAA now encompasses websites offering personalized health management, companies selling dietary supplements or prescription refills and even web-based services that track and store information from glucose monitors, blood pressure cuffs and other devices.

These new types of Covered Entities fall under the jurisdiction of the Federal Trade Commission, while the traditional types still answer to the Department of Health and Human Services (HHS).

The major areas affected in existing HIPAA regulations, with varying effective dates, pertain to security breaches and enforcement.

## **SECURITY BREACHES**

Covered Entities had previously been required to mitigate harm caused by unauthorized disclosures of PHI, but not required to notify individuals whose information was disclosed. Under ARRA, Covered Entities are now required to give notice to individuals whose PHI has been accessed, acquired or disclosed due to a breach.

ARRA defines a breach as the unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the security or privacy of such information. ARRA's definition of "breach" is important because the notification requirements are only triggered in the event of a breach of unsecured PHI, which is information not protected through technology or methods designated by the federal government.

Generally, notification of a breach must be provided "without unreasonable delay," or within 60 days after the discovery of the breach. Notice of a breach may be delayed if law enforcement officials determine that notification would hinder a criminal investigation or violate national security.

In addition, if a breach involves 500 or more individuals, immediate notice must be given to the HHS and prominent media outlets in the applicable state or jurisdiction. The Secretary of Health and Human Services will post a list of Covered Entities involved in the breach on the HHS website. However, if a breach involves 10 or more individuals whose contact information is out of date or deficient, notification must be posted to the Covered Entity's website and also disclosed to major print or broadcast media.

All breach notifications must contain:

1. A description of the occurrence, including the date of the breach and the date of its discovery (if known)
2. A description of the types of unsecured PHI involved in the breach (Social Security number, date of birth, address, account number, etc.). How individuals should protect themselves from potential harm as a result of the breach
3. A description of what is being done to investigate the breach, mitigate losses and protect against further breaches
4. Contact points for individuals to ask questions or receive additional information (toll-free telephone number, email address, website, postal address, etc.)

As required by ARRA, there are two means by which PHI can be rendered unusable, unreadable or indecipherable to unauthorized individuals:

1. Encryption – Proper encryption depends on the strength of the encoding algorithm to make information unreadable, and the security of the decryption process that makes the information readable to the proper parties using a cryptographic key.
2. Destruction – Hard copies of PHI must be shredded or destroyed in a way that renders the PHI unreadable or unable to be reconstructed. Electronic PHI must be cleared, purged or destroyed according to the standards described in the National Institute of Standards and Technology Special Publication 800-88, leaving PHI unretrievable.

## **ENFORCEMENT**

Previously, HIPAA violations could impose a maximum civil monetary penalty of \$100 per violation and up to \$25,000 for all similar violations in a calendar year. Certain wrongful disclosures of PHI could be criminally prosecuted by the Department of Justice and may have been subject to criminal penalty fines of up to \$250,000 and up to 10 years in prison. In addition, HIPAA did not permit individuals to obtain monetary damages for violations, and enforcement was handled at the federal level.

ARRA significantly strengthens HIPAA's penalty and enforcement provisions. The financial penalties have been increased, and a percentage of the civil penalties collected will be distributed to individuals harmed by the violations. Under ARRA, each civil violation of the HIPAA rules may result in penalties ranging from \$100 to \$50,000, while similar violations occurring in a calendar year may result in penalties ranging from \$25,000 to \$1,500,000.

Other changes added by ARRA include:

1. The Secretary of Health and Human Services is authorized to conduct periodic audits of Covered Entities to ensure compliance. The Secretary may also use civil enforcement provisions even if the action in question violates criminal provisions, provided that no criminal conviction is associated with the case. The Secretary is required to

- impose civil penalties if a violation is due to willful neglect, and to formally investigate any complaint if a preliminary investigation indicates the potential of violation due to willful neglect.
2. The Office for Civil Rights is authorized to conduct investigations and impose civil monetary penalties against any individual for criminal violations of HIPAA if the Department of Justice has not prosecuted the individual. Violations due to willful neglect require formal investigation and imposition of civil monetary penalties. The Office will receive any civil monetary penalties or settlements related to HIPAA security-related offenses. Such funds will be used to fund the further enforcement of ARRA and HIPAA rules and requirements. The Secretary is to issue regulations within 18 months of ARRA's enactment to implement this change.
  3. State Attorneys General are authorized to bring civil actions in federal court seeking injunctions or damages against individuals who violate HIPAA, as well as attorney fees. Damages are limited to \$100 for each violation of HIPAA and \$25,000 for similar violations in a calendar year. ARRA also gives power to state Attorneys General to institute legal action to obtain damages on behalf of state residents who have been threatened or adversely affected by HIPAA violations. The only instance in which a state Attorney General may not bring an action is if a federal action is already pending.
  4. Within 18 months of ARRA's enactment, the Comptroller General in the Government Accountability Office is to recommend to the Secretary a method by which individuals who are harmed by violations of HIPAA would receive a percentage of the civil monetary penalties or monetary settlements collected. The Secretary is required to establish by regulation the implementation of this methodology within three years of ARRA's enactment.

## **ELECTRONIC HEALTH RECORDS**

An electronic health record is an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized healthcare clinicians and staff.

In 2004, President George W. Bush issued an Executive Order that required HHS to study and develop a national health information network (NHIN) within a deadline of ten years. The task of overseeing the system was given to a newly created HHS office, The Office of the National Coordinator for Health Information Technology.

When President Obama's ARRA was passed, it called for up to \$19 billion to meet the goal of electronic health records for all Americans – also by 2014.

While the NHIN will not be a reality for several years, many state governments have appointed boards and task forces to study the issue. The initial objective is the creation of a regional network to combine electronic health records from various unrelated sources, followed by the consolidation of several regional networks into a statewide system. Ultimately, the state networks will feed into the national network.

Many factors have fed the public's concern about the potential privacy risks associated with having personal data stored in electronic format. HIPAA's shortcomings, health data accessed by hackers and information lost on laptop computers all add to the trepidation.

## **EFFECTIVE DATES**

Most provisions will be effective one year after the date of ARRA's enactment (February 17, 2010), unless specifically noted. However, the enforcement provisions, such as increased fines and state Attorney General involvement became effective immediately following the date of enactment, February 17, 2009.

Organizations subject to the rule should take the extra time to assess their compliance needs and implement their plans in advance of the deadline.



Business Records Management LLC  
412.321.0600 • 877.342.5276  
[www.businessrecords.com](http://www.businessrecords.com)