



## The American Recovery and Reinvestment Act of 2009

### **A Quick Guide to Navigating the Privacy and Security Provisions of the American Recovery & Reinvestment Act of 2009 November 25, 2009**

*Provided by the HIMSS Privacy and Security Toolkit Work Group*

#### **1. Background:**

On February 17, 2009, President Barack Obama signed into law the **American Recovery and Reinvestment Act of 2009, H.R. 1 (ARRA)**.

Within ARRA, the provisions relating to health information technology are in a section entitled, "Health Information Technology for Economic and Clinical Health" which is commonly referred to as the "HITECH Act." The HITECH Act contains many new laws relating to the use and disclosure of protected health information (PHI). This Act also includes the privacy and security provisions.

#### **2. Some helpful tips to achieve a better understanding of the ARRA legislation:**

The HIMSS Privacy and Security Toolkit Work Group, a group of HIMSS member volunteers, has provided in this paper some "tips" as you and your organization navigate the privacy and security provisions of the HITECH Act. The members of the WG hope that you will find this information helpful and welcome your comments and questions.

##### **2.1 Read the statute in its original form and reference back to it as the source of truth.**

Even if you have another trusted source or reference, your best bet is to always check back with the original statutory language to verify your source's consistency with the original bill.

The following information will help you access the relevant portions of the bill:

- The text of the entire ARRA bill may be found at: [ARRA, H.R. 1](#)
- The text of the HITECH Act may found at: [TITLE XIII: Health Information Technology](#).
- Within the HITECH Act, the Privacy and Security provisions are contained in: TITLE XII: Health Information Technology, [Subtitle D, Privacy](#).

A Quick Guide to Navigating the Privacy and Security Provisions of ARRA. This document is for informational purposes only, and none of its content should be construed as legal advice. HIMSS members are strongly encouraged to independently consult with legal counsel. ©2009 Healthcare Information and Management Systems Society (HIMSS).

## 2.2 Don't depend entirely on abstracts and synopses of the statute.

Abstract and synopses published immediately after the passage of the bill may (and often do) contain discrepancies or inaccurate information due to the haste in which they were produced. Look for publications with recent dates and/or that are updated frequently.

- HIMSS maintains an entire section of its website dedicated to helping its members stay abreast of the statutory and regulatory requirements of ARRA: [Economic Stimulus for the Healthcare Industry](#).

## 2.3 Understand that the ARRA statutory language requires regulations to be written for implementation.

Many of the provisions in the statute require the development of **regulations** to specify implementation requirements. The Statute mandates **what** should occur at a very high level. These mandates are then referred to the appropriate federal department for implementation. The Department of Health and Human Services (HHS) is charged with the development of the regulations and other information that will specify **how** the requirements should be implemented and the associated timeline.

The following regulations and/or guidance are required to be promulgated by HHS. (Section numbers refer to the relevant section of H.R. 1, Section XIII, [Subtitle D, Privacy](#).)

**NOTE: Some of these regulatory and guidance activities are already underway.**

HIMSS members (only) may reference the following HIMSS document for up-to-date information on the regulatory timeline:

[Privacy Provisions: Guidance and Rule Making: Chronological Listing of Key Dates](#)

- **Guidance on Methodologies and Technologies that Render Information Unreadable:** HHS will issue guidance on methodologies and technologies that render information unreadable, as it relates to safe harbor or exemption from the breach notification requirement (Section 13402).
- **HHS Breach Notification Rule:** HHS will promulgate interim final regulations on Breach Notification (Section 13402).
- **FTC Breach Notification Rule:** The Federal Trade Commission (FTC) will develop the regulations and implementation specifications for the Breach Notification requirements that fall under its purview. The FTC rules will apply to breach notification by vendors of Personal Health Records (PHRs) that are not covered by HIPAA or Business Associate agreements (Section 13402, 13407). PHRs are broadly defined as "online repositories of health

information that individuals can create to track their medical visits, prescription information, etc.”<sup>1</sup>

- **Standards and Regulations for Accounting of Disclosures:** HHS will adopt through rulemaking the initial prioritized set of standards which should include the accounting for disclosures (Section 3002b).
- **Guidance on De-Identification of Protected Health Information:** HHS will report on and provide guidance on de-identification of PHI (Section 13424c).
- **Rule on Fundraising:** HHS will issue rules on opting out of fundraising solicitations (Section 13406).
- **Guidance on Effective Technical Security Safeguards:** HHS will report on guidance on the effective technical safeguards for carrying out the HIPAA security rule (Section 13401c).
- **Clarification on Application of Criminal Penalties:** HHS and the Office for Civil Rights (OCR) will clarify the application of criminal penalties for non-covered entities (Section 13409).
- **Regulations on Business Associate Entities:** HHS will issue rules on which entities are required to be business associates (Section 13401).
- **Guidance on Minimum Necessary:** HHS will publish guidance for healthcare organizations on determining the minimum necessary data when a disclosure of PHI is requested (Section 13405c).
- **Regulations Regarding Sale of Data:** HHS will publish regulations regarding the new statutory prohibition on the sale of PHI (Section 13405a).
- **Clarification of Ability to Pursue Civil Penalties:** HHS will issue a clarification on the ability to pursue civil penalties when criminal penalties are not pursued (Section 13405).
- **Regulations for distributing Money Gained from Monetary Penalties:** HHS will issue regulations regarding the methodology for distributing penalties or settlement money to harmed individuals (Section 13410).

---

<sup>1</sup> Federal Register August 25, 2009, Federal Trade Commission 16 CFR Part 318 Health Breach Notification Rule; Final Rule <http://www.ftc.gov/os/2009/08/R911002hbn.pdf>

## 2.4 Get involved and provide your expertise in the regulatory process.

There are many avenues available for input into the regulatory process.

- Avail yourself of the public hearings, teleconferences, webinars, and other activities. Reference the following websites:
  - [HHS Federal Advisory Committee Page](#)
  - [HIMSS ARRA/Economic Stimulus Resource Page](#)
  - [HIMSS Economic Stimulus Education Program Page](#)
- Respond to Public Comment periods. Utilize the [Federal eRulemaking Portal](#) to determine public comment periods, submit comments or review/inspect submitted comments.
  - The HIMSS Privacy and Security Steering Committee and HIMSS Staff solicit and organize member comments for submission. For a list of upcoming rule making activity, please reference the links in section 2.4.1. Contact Lisa Gallagher at [lgallagher@himss.org](mailto:lgallagher@himss.org) or Mike Kroll at [mkroll@himss.org](mailto:mkroll@himss.org) for more information.

### 2.4.1 Keep up to date with the process.

HIMSS maintains a schedule of regulatory activity for its members:

- General:  
[ARRA Chronological Listing of Key Dates](#) (members only)
- Privacy and Security:  
[Privacy Provisions: Guidance and Rule Making: Chronological Listing of Key Dates](#) (members only)

## **APPENDIX A: GLOSSARY**

### **Guidance<sup>2</sup>**

A document such as a book, pamphlet, etc., giving information, instructions, or advice.

### **Regulation<sup>3</sup>**

After Congressional bills become laws, federal agencies are responsible for putting those laws into action through regulations. The types of regulations include: Notices from the Federal Register; Proposed Rules; Final Rules. Documents such as public comments and supporting materials are often associated with these regulations.

### **(Rule and) Rulemaking<sup>3</sup>**

A type of regulation that establishes a **rule**, the means by which congressional laws are implemented.

### **Rulemaking Process<sup>3</sup>**

The process federal agencies use to formulate, amend or repeal a regulation. This process often contains a proposed rule and a final rule, and may accept public comments during specified time periods.

### **Statute<sup>4</sup>**

*Law.*

- a. an enactment made by a legislature and expressed in a formal document.
- b. the document in which such an enactment is expressed.

---

<sup>2</sup> [www.dictionary.com](http://www.dictionary.com)

<sup>3</sup> Federal Rulemaking Glossary accessed at: <http://www.regulations.gov/search/Regs/home.html#glossary>

<sup>4</sup> [www.dictionary.com](http://www.dictionary.com)