Analysis of Health Care Confidentiality, Privacy, and Security Provisions of The American Recovery and Reinvestment Act of 2009, Public Law 111-5

March, 2009

On Tuesday, February 17, 2009, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA), also known as Public Law111-5. Included in the Act are numerous provisions affecting Health Information Management including health information technology (HIT) incentives, education and training for a work force to facilitate implementation and maintain health information communications and technology (HICT), and a number of new privacy provisions.

An analysis of these HIT provisions can be found at www.ahima.org/dc. The purpose of this analysis is to examine the provisions of ARRA specifically addressing the "privacy" of healthcare data.

An electronic copy of ARRA can be found at the Government Printing Office web site: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.txt.pdf. The ARRA text is 407 pages and addresses a myriad of economic stimulus provisions. The provisions affecting healthcare privacy begin on page 144, Subtitle D – Privacy.[1]

ARRA is a law, not a regulation. Some of the provisions written in the law will be directly effective and verbatim, while other parts will require interpretation, regulation, or guidance, and the ARRA spells these out. Because this is a law some of the provisions may be difficult to comprehend. An immediate response or reaction to any of them at this time would be unwise until more clarity exists on intent, or regulation or guidance is issued. Recent meetings with federal officials from the Office of the National Coordinator for HIT (ONC), the Office for Civil Rights (OCR), and the National Committee for Vital and Health Statistics (NCVHS) suggests even these affected government offices, agencies, and advisory commissions have yet to comprehend all of the implications and changes that will be needed.

This analysis describes what is known at this time. AHIMA publications including the weekly *e-Alert*, the *Journal of AHIMA*, and the AHIMA website www.ahima.org should be monitored on a regular basis for more information as it is released. The US Department of Health and Human Services (HHS), the Centers for Medicare and Medicaid (CMS – which oversees HIPAA security compliance, and the OCR (which oversees HIPAA privacy compliance) will be issuing bulletins and other information over time. Those items in ARRA requiring regulation will of course follow the usual

[1] In this document any page reference, enclosed in brackets [ ], refers to the pages in the ARRA copy located at the Government Printing Office Website referenced above.

pattern of notices of proposed rulemaking (NPRM), deliberation, and then the issuance of a final rule. All NPRMs and final rules will be published in the *Federal Register*.

Key Highlights of ARRA Related to Healthcare Privacy

- The ARRA law was developed over several months by Congress and signed by the President on February 17, 2009 – the effective date.
- The Office of the National Coordinator for Health Information Technology (ONC) is codified and advisory committees for policy and standards established. The Coordinator, along with the two committees, a to-be-named chief privacy officer, and existing HIPAA related agencies will be addressing both the changes required by ARRA as well as other confidentiality, privacy, and security issues and standards identified as part of their process in the future.
- ARRA has several provisions that extend HIPAA privacy, security, and administrative requirements to business associates (BAs). In addition there are new provisions for HIPAA-covered entities and BAs, as well as provisions for those not considered HIPAA-covered.
- Breach requirements (identification and notification) are established both for HIPAA-covered entities and non-HIPAA-covered entities, essentially any organization holding personal health information.
- The Act calls for HHS regional office privacy advisors and an education initiative on the uses of health information.
- Restrictions are further established on the sales of health information.
- A new accounting requirement is established for disclosure related to treatment, payment, and operations.
- New access requirements are established for individuals related to healthcare information in electronic format.
- New conditions are instituted for marketing and fundraising functions.
- Personal health record information with non-HIPAA entities is now protected.
- Use of de-identified data and "minimum necessary" data will be addressed.
- Enforcement is improved and penalties are increased.
- The HHS Secretary and the Federal Trade Commission are required to provide a number of reports to Congress and guidance to the entities who are involved with healthcare data.

Effective and Compliance Dates

This Act was signed into law by President Barack Obama on February 17, 2009. Various compliance and reporting dates are expressed throughout the Act and will be highlighted in the analysis below. The Act calls upon the Secretary of HHS and the Coordinator of ONC to perform a number of actions and functions. [*What is unique regarding this Act at this time, is both positions of Secretary and the Coordinator are, at signing, vacant of political appointments. It, therefore, becomes possible that some of the compliance dates spelled out in the Act my slip in timeliness or need to be amended.*]

ARRA Provision Affecting Health Information Communications and Technology (HICT)

Within ARRA are several sections affecting the development and use of health information. Monies have been provided to states, Indian tribes, and federal agencies to expand the use of HICT within their jurisdiction. Several sections of ARRA also address expanding the broadband network within the US so more communities can take advantage of HICT and other Internet capabilities. Finally, there are sections of the Act which specifically define incentives for the adoption of HICT.

Title XIII of ARRA, titled "Health Information Technology" [page 112], specifically addresses HICT and quality, the implementation of HICT, workforce education to assist in the implementation,

research and technical assistance, and funding for grants and loans. All of these aspects of ARRA are discussed in AHIMA's analysis of the ARRA which can be found at http://www.ahima.org/dc.

PRIVACY

Within Title XIII of ARRA is Subtitle D – Privacy [page 144]. This analysis addresses this subtitle and the other components of ARRA affecting healthcare privacy, or as some might define it health data confidentiality and security.

Background on Privacy, HIPAA and ARRA

Congress has been addressing healthcare privacy for several decades. In 1996, with the passage of the Health Insurance Portability and Accountability Act (HIPAA), a major emphasis was cast on privacy as it related to electronic health transactions. Congress allowed itself three years to further develop federal law with regard to healthcare privacy, with the caveat that the HHS Secretary should move forward with regulation in the absence of Congressional Action. Congress did not act, and the Secretary did act culminating in a December 2000 final HIPAA privacy rule posted in the last month of the Clinton administration. The incoming Bush administration did put a hold on the rules, but eventually released the rule, which was later amended. The HIPAA privacy rule finally went into effect on April 14, 2003, except for HIPAA-defined small health plans which had until April 14, 2004 to comply. The OCR is the designated enforcement agency for the HIPAA privacy regulations. The US Department of Justice (DOJ) handles any criminal prosecution.

HIPAA also has a security component whose final rule was not published until February 20, 2003; five years after the proposed rules were published. The security rule's compliance date for all but small health plans was April 21, 2005. Small health plans had a compliance date of April 21, 2006. CMS was designated by the Secretary as the overseer of the security rules.

With the exception of additional enforcement information the security and privacy rules have not been amended since their final rules were published. While the federal government proceeded with the federal privacy and security rules, many states have promulgated laws and regulations related to privacy and security. HIPAA is often called the "federal floor" for privacy and security and the HIPAA law itself does not preempt state law when the state law can be shown to hold compliance to a higher standard. This lack of preemption, along with the fact there are differences and variations of law across the 50 states and other jurisdictions along with other federal laws and regulations, has caused significant problems for those who are covered or must ensure compliance with this myriad of federal and state laws and regulations.

Since the time of HIPAA implementation the healthcare industry has accelerated the adoption and use of electronic health records (EHRs) and electronic health information exchange (HIE). The industry has also experienced an increase in incidences of health information breaches (paper and electronic) and identity theft has also increased and become seemingly reported on an on-going basis. During this time these HIEs, also called Regional Health Information Organizations (RHIOs), along with "health record banks," and personal health record (PHR) vendors have expanded in different models across the country.

Since HIPAA was introduced PHRs have been promoted and developed into a variety of different products. PHRs include:

- Those offered by HIPAA covered entities;
- Self-contained products operated by the consumer;
- PHRs operated by a third party (again in various forms) with data provided by the consumer; and
- "Health record banks," where an entity stores information from a variety of entities related to the consumer and where disclosure is only at the direction of the consumer.

All of these entities, HIEs, RHIOs, and PHR operators handle identifiable personal health information, but many are not covered by HIPAA because the entity is not a HIPAA "covered entity." Some of these entities are covered to some extent by state law or by federal law administered by the Federal Trade Commission. The laws that have been developed have not necessarily kept pace with technological advances.

These environmental changes have caused some individuals and consumer privacy groups, to become concerned about the "privacy" of their health information. Pressure has risen on Congress to address the issue of health information privacy especially in an electronic information world. It is likewise clear, there is no one hundred percent agreement on what constitutes privacy of healthcare data or how privacy should be addressed in the current environment of new technology and a desire to improve population health through the use of aggregate health data.

Congress has continued to grapple with these privacy concerns over the past several years. Each time HIT legislation has been offered, privacy disagreements have stopped the legislation in its tracks. Debates in Congress on the privacy language included in what is now ARRA occurred, publically and privately, in late fall and the early weeks of January. The privacy language and approach in ARRA represents a compromise by the Congress to increase privacy protections while in the eyes of the language developers providing a mechanism for further adoption of HICT.

ARRA Privacy Section Organization

The privacy provisions in ARRA are somewhat scattered throughout the Act. This Analysis approaches some of the content collectively rather than in the order they appear in the Act. **Attachment A** provides a reference to the order of the privacy and security references as they are noted in the actual Act.

Privacy, ONC and the Future of Healthcare Privacy and Security

ARRA codifies the Office of the National Coordinator for HIT, a goal of AHIMA for several years. ARRA also establishes an organization to address the adoption, implementation, and use of EHRs and HIEs. Privacy and security are also addressed in this codification. This organization can be anticipated to provide additional confidentiality, privacy, and security standards, regulations, and guidance in the future.

[*Note: Any reference to Coordinator should be assumed to mean the Coordinator overseeing ONC, and unless otherwise indicated "Secretary" refers to the Department of Health and Human Services Secretary.*]

ONC

Under Subtitle A – Promotion of Health Information Technology, Section 3001 [page 116] – Office of the National Coordinator for Health information Technology, Congress calls for ONC to update the Federal Health IT Strategic Plan to include specific objectives, milestones and metrics, including:

- "The incorporation of privacy and security protections for the electronic exchange of an individual's individually identifiable health information;" and
- "Ensuring security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable."

The strategic plan is required to be measurable and the plan and its progress are to be posted on the ONC website, http://www.hhs.gov/healthit/, for public observation.

Under Section 3001, the Secretary of HHS is required [page 119] to appoint a "Chief Privacy Officer of the Office of the National Coordinator, within 12 months (February 17, 2010), whose duty it shall be to advise…on privacy, security, and data stewardship of electronic health information and to coordinate with other Federal agencies (and similar privacy officers in such agencies), with State and regional efforts, and with foreign countries with regard to the privacy, security, and data stewardship of electronic individually identifiable health information."

[*Note: the law does not spell out exactly how the role of the new ONC Chief Privacy Officer will relate to the OCR or CMS, but no enforcement powers are given and therefore it must be presumed this role will be advisory similar to existing ONC staff who have been working in the area of confidentiality, privacy, and security for several years.*]

HIT Policy Committee

An HIT Policy Committee is established, Section 3002 [page 120], to make policy recommendations to ONC relating to the implementation of a nationwide health information technology infrastructure, including implementation of the strategic plan.

Among the areas for infrastructure standards, the Policy Committee is to consider:

- "Implementation specifications shall include named standards, architectures, and software schemes for the authentication and security of individually identifiable health information and other information as needed to ensure the reproducible development of common solutions across disparate entities."
- "Technologies that protect the privacy of health information and promote security in a qualified electronic health record [see below] including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns, in accordance with applicable law and for the use and disclosure of limited data sets of such information." [Note: *The references here relate to later language dealing with segmentation and limited data sets. These issues will be under considerable discussion and review in the months to come.*]
- "Technologies that allow individually identifiable health information to be rendered unusable, unreadable, or indecipherable to unauthorized individuals when such information is transmitted in the nationwide health information network or physically transported outside of the secured, physical perimeter of a health care provider, health plan, or health care clearing house." [page 121]

Other areas of the Policy Committee consideration relate to the use of quality data and public health, medical and clinical research, and drug safety, as well as technologies that facilitate the use and exchange of patient information and "reduce wait times."

Members of the Policy Committee [page 122] are appointed by the HHS Secretary, Congressional Leadership, and the Comptroller General of the US. Included in the Comptroller General's appointments is one member with "expertise in health information privacy and security." [*Note: The members of this Committee are to be appointed within 45 days of the February 17, 2009 enactment. If Congress or the Comptroller General do not appoint within this time, the Secretary of HHS is permitted to make the appointment.*]

The provision for membership [page 123] also notes the Committee shall ensure an opportunity for the participation in activities of the committee of outside advisors, including individuals with expertise in the development of policies for the electronic exchange and use of health information, including in the areas of health information privacy and security.

HIT Standards Committee
Section 3003 [page 124] establishes a HIT Standards Committee to recommend to ONC standards, implementation specifications, and certification criteria for the electronic exchange and use of health information. This committee is to be appointed with the National Coordinator taking "a leading position in the establishment and operations of the Committee," and within 90 days of enactment of ARRA is to develop a schedule for the assessment of policy recommendations from the Policy Committee. This schedule is to be updated annually.

The membership of the Standards Committee is to come [page 125] from government and private sectors and include "individuals with technical expertise on health care quality, privacy, and security, and on the electronic exchange and use of health information. The Standards Committee is also to include "outside involvement" including individuals with expertise in health information privacy and security.

Miscellaneous Provisions – Relation to HIPAA and Flexibility
Section 3009 [page 128] specifies that with respect to the ARRA relationship to HIPAA privacy and security, nothing in ARRA should be construed as having any effect on the authorities of the Secretary provided under HIPAA, and any standards developed under ARRA must take into account the requirements of HIPAA privacy and security law. This section also gives the Secretary authority to modify the Act's definition of health care provider [Section 3000 (3), page 114] when appropriate.

ARRA Privacy Provisions

Definitions – Title VIII
While Subtitle D provides a number of definitions, there are definitions made earlier in Title XIII, Section 3000 [pages 114-115], that are referred to in the Privacy sections which follow. Section 3000 also notes a number of definitions coming from and shared with the HIPAA law. So, unless noted below assume a HIPAA definition. Included in these Section 3000 definitions are:

- **Certified EHR Technology** means a qualified EHR which is certified under conditions established in Title XIII and applicable to the type or record involved.

- **Health Care Provider** includes [*some defined in other specific legislation*]: hospital, skilled nursing facility (SNF), nursing facility, home health entity, or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center [more than one site], emergency medical services provider, federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician, a practitioner, a provider related to an Indian tribe or organization [several sites], a rural health clinic, a covered entity, and "any other category of health care facility, entity, practitioner or clinician determined by the Secretary.
- **Health Information Technology** means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by healthcare entities or patients for the electronic creation, maintenance, access, or exchange of health information.
- **Qualified Electronic Health Record** means an electronic record of health-related information on an individual that:
    - Includes patient demographic and clinical health information, such as medical history and problem lists; and
    - Has the capacity to:
        - Provide clinical decision support;
        - Support physician order entry;
        - Capture and query information relevant to health care quality, and
        - Exchange electronic health information from other sources.

Subtitle D – Privacy Definitions

Again, many of the definitions used in this section come from sections of the HIPAA law or 45 CFR Parts 160 through 164, unless otherwise noted. The privacy definitions are included under Section 13400 [page 144-145] of ARRA and include:

- **Breach** [see discussion of breach below]
- **Covered Entity which** has the meaning given in HIPAA Section 160.103 meaning a health plan, a healthcare clearing house, or a health care provider which transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulation. [*We will use the abbreviation CE when referring to a HIPAA covered entity, unless otherwise noted.]*
- **Electronic Health Record** means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
- **Personal Health Record [PHR]** means an electronic record of PHR identifiable health information [see below] on an individual that can be drawn from multiple sources and is managed, shared, and controlled by or primarily for the individual.
- **Vendor of Personal Health Records** means an entity, other than a CE, that offers or maintains a PHR.
- Since the term **Protected Health Information (PHI)** is used quite a bit in the document, we remind readers that HIPAA (160.103) defines this term as meaning individually identifiable health information that is
    - transmitted by electronic media;
    - maintained in electronic media; or
    - transmitted or maintained in any other form or medium

    Excluded from this definition are education records covered under the Family Educational Rights and Privacy Act, Sections of the Higher Education Act, and employment records health by a HIPAA CE in its role as an employer.

Part 1 – Improved Privacy Provisions and Security Provisions

Subpart D is divided further into two parts; this first part, and a second that deals with the relationship of this subpart with other laws and regulations, effective dates, and reports. This part, as noted above, divides some of the subject matter into non-congruent sections. For the sake of understanding, we will deal with the subject matter as one and note the sections of the law that are under discussion.

Business Associates (BAs)

BAs – Application of Security Provisions
Section 13401 [page 146] applies several of the HIPAA security provisions to Business Associates of HIPAA CEs. These include:

- HIPAA Section 164.308 – Administrative Safeguards;
- HIPAA Section 164.310 – Physical Safeguards;
- HIPAA Section 164.312—Technical Safeguards; and
- HIPAA Section 164.316—Policies and Procedures and Documentation Requirements

In addition to BAs now being required to be in compliance with these HIPAA sections, the Business Associate Agreement (BAA) is required to incorporate these new provisions in to the agreement between the BA and the CE.

The BA is also subject to the civil and criminal penalties associated with violating any of the security provisions "in the same manner such sections apply to a CE that violates such security provisions."

ARRA Section 13401 also notes for the first year after enactment and annually thereafter, the Secretary shall, "after consultation with stakeholders," annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the security sections noted above.

Section 13404 [page 150] then addresses the **Privacy Provisions and Penalties to Business Associates of HIPAA covered entities**. These include:

- The section, Application of Contract Requirements, first notes that any BA of a CE that receives PHI under HIPAA [*Uses and Disclosure of Protected Health Information: General Rules – Standard for Disclosures to Business Associates*[2] *and the Standard for Business Associate Contracts*[3]] must now under ARRA, apply the new requirements of ARRA as well.
- A second section, Application of Knowledge Elements Associated with Contracts, essentially makes the acknowledgement of non-compliance a two-way proposition. Whereas HIPAA required a CE to note any privacy non-compliance of the BA, and was required to either have the BA correct the situation, or drop the BA, this new ARRA section requires that the BA also respond to privacy non-compliance on the part of the CE in the same manner.
- The third provision in Section 13404, Application of Civil and Criminal Penalties, notes that a BA that is non-compliant with the first two provisions in this section is also subject to the same civil and criminal penalties as the CE.

[2] Section 164.502 (e) (2)
[3] Section 164.504 (e)

Business Associate Contracts Required for Certain Entities
Section 13408 provides that each organization (HIE, RHIO, PHR operator, or E-Prescribing Gateway) with respect to a CE, that provides data transmission of PHI to the CE or its BA and that requires PHI access on a routine basis is required to enter into a written contract (or other written arrangement) described in the HIPAA section on disclosure to BAs[4] as well as the HIPAA section on administrative safeguards[5] in relation to BA contracts and other arrangements. Effectively, then these organizations will be required to become a BA of associated CEs, and accountable under both the requirements of HIPAA as well as those applied to BAs in ARRA.

Breach

Definition – Breach
The definition of "breach" covered in section 13400 (definitions – page 144) must be understood since it could conflict with other definitions of breach that are included in state laws or regulations. In the privacy section of ARRA breach is defined as follows:

- IN GENERAL – The term "breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
- EXCEPTIONS – The term "breach" does not include:
    - Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a CE or BA if:
        - Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the CE or BA; and
        - Such information is not further acquired, accessed, used, or disclosed by any person; or
    - Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person."

[*Note: CEs or BAs will have to take note of the person/employee involved and whether his or her position or function is within the scope of the employment or professional relationship as defined by organization policy or practice.*]

Definition – Unsecured Protected Health Information
The definition of "unsecured protected health information" is covered in Section 13402 (notification in the case of breach – pages 148-149).

Essentially "unsecured protected health information" means PHI that is not secured through the use of a technology or methodology specified by the Secretary in the guidance also required in this Section. However, if the Secretary does not release this guidance by the required date, the definition of "unsecured protected health information" then means PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed

[4] Section 164.502
[5] Section 164.308 (b)

or endorsed by a standards developing organization that is accredited by the American National Standards Institute (ANSI).

Guidance for Technology to Secure Protected Health Information
The guidance referenced in Section 13402 is required from the Secretary, after consultation with stakeholders, within 60 days after enactment [page 149].

Notification in the Case of Breach
Section 13402 [pages 146-149] covers the notifications required when this new federal breach requirement is in effect. Note it is possible that for compliance an organization or entity may have to follow both federal and state requirements. The Secretary is required to promulgate interim final regulations within 180 days of the enactment of ARRA, and the requirements in this interim final regulation will become effective 30 days after the date of publication of the interim final regulation. [*Interim final regulations allow comments to be made by the public even though these rules are considered final (and will be affective shortly). This allows the Department to make further changes in the rule, raised by the comments, if necessary. Nonetheless, the rules are intended to be in affect no later than 210 days after the date of enactment.*]

In general, an entity covered by this section (CEs or BAs) that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI must **notify each individual** whose unsecured PHI has been or is reasonably believed by the entity to have been accessed, acquired, or disclosed as a result of a breach, when the breach is discovered by the entity.

A **BA** performing the activities just noted, "shall, following the discovery of a breach of such information, notify the covered entity…" The BA's notice must include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during the breach.

A **breach shall be treated as discovered** by the CE or by a BA on the first day on which the breach is known to the entity or BA – including any person, other than the individual committing the breach, that is an employee, officer, or other agent of an entity or associate, respectively – or should reasonably have been known to such entity or associate (or person) to have occurred. This section sets the stage then for the timeliness of a notification and could be crucial should the CE or BA later be prosecuted for not responding appropriately.

All **notifications must be made** without unreasonable delay and in **no case later than 60 calendar days** after the discovery of a breach by the CE or BA involved. The CE or BA has the burden of demonstrating that all notifications were made as required including evidence demonstrating the necessity of any delay.

A **notice to the individual** whose PHI is involved in the breach must be provided promptly as follows:

- **Written notification** must be made by first-class mail to the individual or next of kin at the last known address of the individual or next of kin, or if specified as a preference by the individual, by electronic mail. Notification may be provided in one or more mailings as information is available. In **cases where urgency is required** because of "possible imminent misuse of unsecured PHI," additional notice can be made to provide information to the individual affected by the breach by telephone or other means as appropriate.

- If there is **insufficient or out-of-date contact information** that precludes direct written or electronic mail communication a **substitute form of notice** must be provided. Where there are more than 9 individuals involved "a **conspicuous posting** for a period determined by the Secretary [should be placed] on the home page of the Web site of the CE involved or notice in major print or broadcast media, including major media in geographic areas where the individual affected by the breach [are] likely to reside." These various notices must include a toll-free phone number where the individual can learn whether or not the individual's unsecured PHI is possibly included in the breach.
- **Notices** are required **to prominent media outlets** serving a State or jurisdiction following a breach when the unsecure PHI affects more than 500 residents of a state or jurisdiction and is or is reasonably believed to have been accessed, acquired, or disclosed during a breach.
- Notice to the Secretary must be made immediately when 500 or more individuals are involved in a breach. The Secretary is required to post a list identifying each CE involved in a breach in which more than 500 individuals are involved.
- When the breach affects less than 500 individuals, the CE may maintain a log of any breach occurring in the year [*not defined at this point*] and annually submit it to the Secretary.

Regardless of the method by which notice is provided to individuals, the **notice of breach must include** [page 148] (to the extent possible):

- A **description of what happened**, including the date of the breach and the date of discovery of the breach, if known.
- A **description of the types of unsecured PHI** that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
- The **steps individuals should take to protect themselves** from potential harm resulting from the breach.
- A brief description of **what the covered entity involved is doing** to investigate the breach, to mitigate losses, and to protect against any further breaches.
- **Contact procedures** for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

In this Section, Congress also requires the Secretary [page 149] to periodically report information regarding breaches to key Congressional Committees including the number and nature of the breaches reported and the actions taken in response to such breaches. [*It is not clear if these actions are those taken by HHS, the CE or BA, or both.*]

Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities

ARRA Section 13407 [page 155-57] addresses breaches as they apply to non-CEs or BAs which are vendors of PHRs or:

- offer products or services through the website of a vendor of PHRs; or
- serves as an entity that is not a CE which offers products or services through the website of a CE offering individuals PHRs; or
- serves as an entity that is not a CE and that accesses information in a PHR or sends information to a PHR; and
- is a third party service provider used by a vendor or entity described immediately above to assist in providing PHR products or services.

The Section requires that following the discovery of a breach of security of such information that is obtained through a product or services provided by one of the above entities the entity shall:

- Notify each individual who is a citizen or resident of the United States whose unsecured "PHR identifiable health information" was acquired by an unauthorized person as a result of a breach of security; and
- Notify the Federal Trade Commission (FTC).

Notification by Third Party Service Providers

A third party that provides services to a vendor of PHRs or to an entity described immediately above in connection with the offering or maintenance of a PHR or a related product or services that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information in a record as a result of such services shall, following the discovery of a breach, notify the vendor or entity, respectively, of the breach. The notice shall include the identification of each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during a breach.

These non-CE vendors must follow ARRA Section 13402 [*described above*] notification requirements in a manner to be specified by the FTC. The FTC will also notify the Secretary of the breach of security.

This ARRA section provides that a violation in these non-CE cases will be treated as an unfair and deceptive act or practice in violation of a regulation under specified sections of the Federal Trade Commission Act.

This section also has specific definitions including:

- **Breach of security** – means, with respect to unsecured PHR identifiable health information of an individual in a PHR, acquisition of such information without the authorization of the individual.
- **PHR Identifiable Health Information** – means individually identifiable health information as defined in HIPAA[6], and includes, with respect to the individual, information:
    - that is provided by or on behalf of the individual and
    - that it identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
- **Unsecured PHR identifiable Health Information** – means either:
    - PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance to be issued under ARRA Section 13402, unless
    - Timely guidance is not issued by the date specified in Section 13402, in which case, for this Section only, it shall mean PHR identifiable health information that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization accredited by ANSI.

The FTC is required to promulgate interim final regulations for this section not later than 180 days after enactment of this section. And the provisions of this section shall apply to breaches of security discovered on or after the date that is 30 days after the date of publication of the final regulations. This ARRA provision also has a Sunset clause; so if Congress enacts new legislation establishing

[6] Section 160.103 (defined here as 42 U.S.C. 1320d(6)

requirements for notification in the case of a breach of security for non-CEs or BAs then this section will not apply on or after the new regulations go into effect.

[*It must be noted this section for non-CEs and BAs is not a modification of the HIPAA rules and the entities affected by this section do not become HIPAA CEs or BAs just by the fact that they are included under ARRA provisions.*]

Education on Health Information Privacy

In Section 13403 [page 149] Congress addresses privacy education programs:

- Within 6 months after ARRA enactment, the HHS Secretary is to designate an individual – a **privacy advisor** – in each regional office of HHS to offer guidance and education to CEs, BAs, and individuals on their rights and responsibilities related to Federal privacy and security requirements for PHI; and
- Within 12 months the OCR must develop and maintain a "**multi-faceted national education initiative** to enhance public transparency regarding the uses of PHI, including programs to educate individuals about the potential uses of their PHI, the effects of such uses, and the rights of individuals with respect to such uses." These programs are to be conducted in a variety of languages and present information in a clear and understandable manner.

Restrictions on Disclosures

Section 13405 [page 150-154] covers a number of provisions. The Section is titled: Restriction on Certain Disclosures and Sales of Health Information; Accounting of Certain Protected Health Information Disclosures; Access to Certain Information in Electronic Format

Requested Restrictions on Certain Disclosures of Health Information
This provision [page 150] relates directly to HIPAA's "Rights to Request Privacy Protection for Protected Health Information[7]," and specifically the standards "Right of An Individual to Request Restriction of Uses and Disclosure[8]" and "Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations."

Under HIPAA, a CE did not have to agree to such a requested restriction. Now under ARRA, a CE must comply with the requested restriction if:

- "Except as otherwise required by law, the disclosure is to a health plan for purpose of carrying out payment of health care operations (and is not for purposes of carrying out treatment);" and
- "The PHI pertains solely to a health care item or service for which the health care provided involved has been paid out of pocket in full."

[*This requirement could pertain to an entire encounter, visit, or admission, or a portion of such an encounter. It will require modification to various administration and clinical health record systems or processes. This provision also means the data can be used for treatment, so any approach must provide for flexibility so the data is available when appropriately needed.*]

[7] Section 164.522
[8] Section 164.522 (i) (A)

Disclosures Required to be Limited to the Limited Data Set or the Minimum Necessary
This provision [page 150-151] related to HIPAA – "Use and Disclosure of Protected Health Information General Rules[9]" – "Minimum Necessary." The Secretary is to issue guidance within 18 months of enactment on what constitutes "minimum necessary" under HIPAA Part 164 E – "Privacy of Individually Identifiable Health Information." The Secretary is to take into consideration guidance related to de-identification also called for in ARRA, and "the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease." In the meantime, when responding to a request for information, a CE is to rely on the "**limited data set**" defined in HIPAA,[10] or if that will not suffice, to make a judgment and provide only the minimum necessary to "accomplish the intended purpose of such use, disclosure, or request, respectively."

[*This changes the approach to "minimum necessary." Under HIPAA (pre-ARRA) there are conflicting requirements related to "minimum necessary," especially in situations outside of treatment, by provisions suggesting minimum necessary should be defined by the requestor (when the requestor is a CE). However, HIPAA also allowed the holder of the information to use best judgment on what to release. Now the data holders' responsibility is clearer, however, it is unclear what form the Secretary's guidance might take. Most commenters have suggested the limited data set does not suffice for many of the requests made under the payment and health operations section of HIPAA.*]

Accounting of Certain Protected Health Information Disclosures Required if Covered Entity Uses Electronic Health Record
Like other provisions in this Section, this provision [page 151-152] relates to a HIPAA rule "Accounting of Disclosures of Protected Health Information[11]. This new ARRA provision calls for:

- A revision to the HIPAA provision[12] such that if a CE uses or maintains an electronic health record, the HIPAA exception for accounting of disclosures for treatment, payment, and health care operations no long applies; and
- An "individual shall have a right to receive an accounting of disclosures…made by the CE during the three years prior to the date on which the accounting is requested."
- The requirement for such a disclosure relies on a timetable depending on when the EHR as defined was or is in use, such that:
    - Those CEs possessing an EHR, as defined, before January 1, 2009, do not have to provide such an accounting on PHI disclosures until January 1, 2014; while
    - Those CEs acquiring an EHR, as defined, on or after January 1, 2009 must provide the required accounting of PHI disclosures on and after the later of the following:
        - January 1, 2011; or
        - The date it acquires an EHR as defined.
    - The Secretary can modify these date requirements, however there are limits to what the Secretary can modify, such that:
        - The date applying to those CEs that had an EHR before January 1, 2009, must not be later than 2016; and
        - Those acquiring an EHR after January 1, 2009, must have a required date no later than 2013.

[9] Section 164.502 (b) (1)
[10] Section 164.514 (e) (2)
[11] Section 164.528
[12] Section 164.528 (a) (1) (i)

- The rule also permits the CE to either account for its own releases and the releases of its BAs, or to allow/require the BA to make its own accounting. BAs are specifically required to respond to individuals' requests if made directly.

The Secretary is directed to promulgate regulations on what information must be collected in order to respond to the requests [*or, if you will, defines what an individual can request in the way of an accounting*]. The Secretary's regulations must come out in six months.

[*This provision has many loose ends surrounding rules, technology, customer service, BA agreements to name a few. These will have to be addressed by the Secretary as requested by Congress. It appears that Congress assumed CEs use an EHR with the same capabilities and processes, or will be using them in the future once vendors understand and incorporate the new requirements into their products.*

EHR purchasers must be alert to this requirement and the resulting requirements as it sets specifications for an EHR purchase. Since not all EHRs are the same, the response to these requirements may have to vary depending on the standards developed and the final regulations.

Just how a CE should deal with the question of whether it or its BAs will respond to a request for disclosures is also difficult to address since BAs' capabilities will also be mixed, and the provision appears to require BAs to respond to direct requests by affected individuals.

It is also open as to how consumers and consumer groups will respond to this provision and the Secretary's rules, given the range of dates Congress has provided for compliance.]

Prohibition on Sale of Electronic Health Records or Protected Health Information

The provision [page 152-154] relates to HIPAA's "Uses and Disclosures for Which an Authorization is Required[13]." Essentially this ARRA provision does not permit a CE or BA to directly or indirectly receive remuneration in exchange for any PHI of an individual unless covered by a valid authorization. Furthermore, the authorization must specify whether the entity receiving the PHI can further exchange the information for remuneration. There are **exceptions**, which include:

- **Public health data** as defined in HIPAA[14]
- **Research data** as defined in HIPAA[15] and the price, if charged, must reflect "the costs of preparation and transmittal of the data for such purpose."
- When "the purpose of the exchange is for the **treatment** of the individual, subject to any regulation that the Secretary may promulgate to prevent PHI from inappropriate access, use, or disclosure."
- When the purpose of the exchange is for **health care operations** specifically[16] activities related to business management and general administrative activities of the entity including the sale, transfer, merger or consolidation of all or part of the CE with another CE, or an entity that following such activity will become a CE and due diligence [is] related to the activity.
- When the purpose of the exchange is for **remuneration that is provided by a CE to a BA** for activities involving the exchange of PHI that the BA undertakes on behalf of and at the specific request of the CE pursuant to a BAA.

[13] Section 164.508
[14] Section 164.512 (b)
[15] Sections 164.501 and 164.512 (i)
[16] Section 164.501

- When the purpose of the exchange is to **provide an individual with a copy** of the individual's PHI pursuant to HIPAA requirements[17] in "Access of Individuals to Protected Health Information."
- When the purpose of the exchange is **otherwise determined** by the Secretary in regulations to be similarly necessary and appropriate.

The Secretary must promulgate rules for this subsection within 18 months of enactment. In doing so, the Secretary must consider the price to be charged for preparation and transmittal of data for public health activities and those conducted by or for the use of the Food and Drug Administration (FDA) and whether charging for such information will impede the research or public health activities.

Once promulgated, the rule will apply to exchanges occurring on or after 6 months from the date of promulgation of the final rule.

Access to Certain Information in Electronic Format
Finally this Section deals with the HIPAA section on "Access of Individuals to Protected Information[18] for situations where the CE uses or maintains an EHR (definition above). It requires:

- That in this situation the individual has the right to obtain a copy of their PHI in electronic format, and if the individual so chooses, to direct the CE to transmit the copy directly to an entity or person designated by the individual provided the request is "clear, conspicuous, and specific; and
- Notwithstanding HIPAA requirements[19] related to fees, the CE may impose a fee for providing the electronic information (or summary) to the requesting individual. The fee is not to be greater than the entity's labor cost in responding to the request for the copy (or summary or explanation).

[*As some readers are aware the issue of copying fees has been contentious and there are a variety of state laws that could possibly conflict with this requirement.*]

Conditions on Certain Contacts as Part of Health Care Operations

Section 13406 [page 154-155] specifically addresses marketing and fundraising.

Marketing
The first provision of this Section [page 154] addresses marketing as part of health care operations and clarifies that "a communication by a CE or BA that is about a product or service that encourages recipients of the communication to purchase or use the product or service shall not be part of health care operations unless the communication complies with subparagraphs i, ii, or iii[20] in HIPAA Section 164.501 – "Definitions." These three subparagraphs come under "marketing" in the HIPAA rule.

---

[17] Section 164.524
[18] Section 164.524
[19] Section 164.524 (c) (4)
[20] HIPAA 164.501 (e) (i) reads: to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of , or enhancements to , a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of a plan of benefits.
HIPAA 164.501 (e) (ii) reads: For treatment of the individual; or
HIPAA 164.501 (e) (iii) reads: for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

ARRA Section 13406 further states: "a communication from a CE or BA covered in these three subparagraphs will not be considered a health care operation if the CE received or has received direct or indirect payment in exchange to making such communication, with the following exceptions:

- The communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication, and
- Any payment received by the CE in exchange for making a communication is "reasonable in amount" and each of the following conditions apply:
    - The communication is made by the CE; and
    - The CE making the communication obtains from the recipient of the communication a valid authorization,[21] and
- Each of the following conditions apply:
    - The communication is made by a business associate on behalf of the CE; and
    - The communication is consistent with the written contract (or other written arrangement described in the HIPAA requirements[22]for disclosures to BAs).

"Reasonable in amount" is to be defined in regulation by the Secretary. "Direct or indirect payment" shall not include any payment for treatment, as treatment is defined by HIPAA.[23]

Opportunity to Opt Out of Fundraising

This provision calls for the Secretary to issue a regulation noting that any written fundraising communication that is considered a "healthcare operation" as defined in HIPAA,[24] shall "in clear and conspicuous manner," provide an opportunity for the recipient of the communications to elect not to receive any further such communication. When the individual elects not to receive any further such communication, the election shall be treated as a "revocation of authorization" as defined under HIPAA.[25]

As written, the requirements of ARRA Section 13406 are to apply to written communications (for marketing and fundraising) occurring on or after one year from the date of enactment of ARRA.

Clarification of Application of Wrongful Disclosure Criminal Penalties

ARRA Section 13409 [page 157] amends Section 1177(a) of the Social Security Act (42 U.S.C. 1320d-6(a)) which deals with the criminal penalties associated with the wrongful disclosure of individually identifiable health information. The amendment states: "For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a CE and the individual obtained or disclosed such information without authorization."

[*Effectively this ARRA section closes the book on a Department of Justice letter that suggested only the CE and not an employee could be pursued for a HIPAA privacy violation or security violation. Recently, DOJ attorneys have found ways to prosecute anyway, but with this new section all*

[21] Section 164.508
[22] Section 164.502 (e)
[23] Section 164.501
[24] Section 164.501
[25] Section 164.508

individuals defined as employees of the CE or BA can be individually prosecuted if they are involved in a violation.]

Improved Enforcement

Section 13410 [pages 157-162] carries a number of items Congress lumped together as improved enforcement. Many of these also relate to Section 1177(a) o f the Social Security Act (42 U.S.C. 1320) which established the penalties as we currently know them.

Noncompliance Due to Willful Neglect
The first provision [page 157] states, "A violation of a provision of this part due to willful neglect is a violation for which the Secretary is required to impose a penalty." For the penalty to be levied, the Secretary must formally investigate any complaint of a violation of a provision of HIPAA privacy; and when the investigation indicates a violation due to willful neglect impose the new penalty. This change will apply to penalties that occur more than 2 years after the enactment date. The Secretary is to publish final regulations related to this requirement not later than 18 months after the ARRA enactment.

Distribution of Certain Civil Monetary Penalties Collected
This provision [page 158] calls for any civil monetary penalty (CMP) or monetary settlement collected with respect to an offense punishable under ARRA privacy provisions or the Social Security Act (HIPAA) to be transferred to the HHS Office of Civil Rights for the purpose of enforcing the provisions of these ARRA provisions or HIPAA. The GAO is to submit a report to the Secretary within 18 months of enactment, with recommendations for a methodology under which an individual who is harmed by an act that constitutes an offense to the ARRA provisions or HIPAA may receive a percentage of any CMP or monetary settlement collected. Then, within 3 years of enactment, the Secretary shall establish regulations based on the GAO recommendations. The methodology will apply with respect to CMPs or monetary settlements imposed on or after the effective date of the regulation.

Tiered Increase In Amount of Civil Monetary Penalties
Again we have a provision [page 158] that modifies the Social Security Act Penalties. In this case a tiered set of penalties is established as follows:

- Where there is a violation where it is established that the person did not know (and by exercising reasonable diligence would not have known) that such person violated a provision, a penalty for each violation will be at least $100 for each violation, not to exceed $25,000."
- Where there is a violation it is established that the violation was due to reasonable cause and not to willful neglect, a penalty for each such violation will be at least $1,000 for each violation, not to exceed $100,000 for each violation.
- Where there is a violation where it is established that the violation was due to willful neglect:
    - If the violation is corrected, a penalty in the about of $10,000 will be required for each violation, not to exceed $250,000.
    - If the violation is not corrected as described, a penalty in the amount of $50,000 will be required not to exceed $1,500.000.

In determining the amount of a penalty under this provision, for a violation, the secretary is to base the determination on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. These penalties apply to violations occurring after the date of enactment.

[*This section on tiers, as it currently appears in the Act, is very confusing and there probably needs to be a correction. We are showing the section as we have seen a consensus of legal observers. We clarify this issue as more information comes forward.*]

Enforcement by State Attorneys General
The provision [page 160] applies to cases where the attorney general of a state has reason to believe the interest of one or more residents of that state has been or is threatened or adversely affected by any person who violates a provision of HIPAA. The attorney general of the state may bring a civil action on behalf of such residents in a district court of the US of appropriate jurisdiction to either enjoin further violation by the defendant, or to obtain damages on behalf of the residents involved.

In these cases the CMP is calculated by multiplying the number of violations by up to $100.00. The total amount of damage imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.00. In assessing damages, the court may consider the same factors that are required of the Secretary in determining the amount of a CMP under HIPAA. In the case of any successful action the court in its discretion may award the costs of the action and reasonable attorney fees.

The state is required to notify the Secretary prior to any action described in this provision and provide the Secretary with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the state must serve notice immediately upon instituting an action. The Secretary has the right:

- To intervene in the action;
- Upon intervening, to be heard on all matters arising therein; and
- To file petitions for appeal.

If the Secretary has instituted an action against a person with respect to ARRA or HIPAA, no state attorney general can bring an action under these provisions.

The provisions stated here apply to violations after the date of enactment.

Corrective Action
The final provision [page 162] notes that nothing in this Section is to be construed as preventing the OCR from continuing, in its discretion, to use corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) of the violation involved.

Audits

Section 13411 [page 162] requires the Secretary to perform periodic audits to ensure CEs and BAs, subject to HIPAA and now ARRA, are complying with all requirements in effect.

Part 2 – Relationship to Other Laws; Regulatory References; Effective Date; Reports

Relationship to Other Laws

Section 13421 [page 162] is very brief and notes the following:

- **Application of HIPAA State Preemption** – the provisions of HIPAA that apply to state preemption apply to these ARRA provisions as well.
- **Health Insurance Portability and Accountability Act** – the standards governing the privacy and security of individually identifiable health information in HIPAA remain in effect to the extent they are consistent with ARRA. The Secretary must by rule amend any federal rule as required to make such regulations consistent with ARRA.
- **Construction** – nothing in ARRA shall constitute a waiver of any privilege otherwise applicable to an individual with respect to the PHI of such individual.

Regulatory References and Effective Date

Section 13422 [page 162] – Regulatory References – notes that any reference to a Code of Federal Regulations refers to such provisions in effect on the date of the enactment of ARRA. Essentially for this Privacy section, the Code refers to either the HIPAA regulations or the Social Security Act requirements related to HIPAA and now ARRA enforcement.

Section 13323 [page 162] – **Effective Date – notes that except as otherwise provided, the provision of Part 1 [the ARRA Privacy Sections] shall take effect on the date that is 12 months after the date of the enactment of ARRA.**

Studies, Reports, Guidance

Section 13424 [pages 164] identifies a number of studies, reports, and guidance required as a result of Part 1. These are as follows.

- **Report on Compliance** – The Secretary is required to provide an annual public report to the Senate Committee on Health, Education, Labor, and Pensions (HELP) and the House of Representatives Ways and Means (W&M) and Energy and Commerce (E&C) Committees related to complaints of alleged violations of law, covering both ARRA and HIPAA security and privacy. The report must include:
    - The number of complaints;
    - The number of complaints resolved informally, a summary of the types of complaints and the number of CEs that received technical assistance from the Secretary during the year in order to achieve compliance and the types of compliance provided;
    - The number of complaints that have resulted in the imposition of civil monetary penalties or have been resolved through monetary settlements, including the nature of the complaints involved and the amount paid in each penalty or settlement;
    - The number of compliance reviews conducted and the outcome of each review;
    - The number of subpoenas or inquires issued;
    - The Secretary's plan for improving compliance with and enforcement of provisions for the following year; and

- The number of audits performed and a summary of audit findings as now required in ARRA.

- **Study and Report on Application of Privacy and Security Requirements to Non-HIPAA Covered Entities** – within the year after enactment the Secretary, in consultation with the FTC, must conduct a study and submit a report to HELP, W&M, and E&C on privacy and security requirements for entities that are not covered entities, or business associates as of the date of enactment of ARRA. The report should include:
  - Requirements relating to security, privacy, and notification in the case of a breach of security or privacy (including the applicability of an exemption to notification in the case of individually identifiable health information that has been rendered unusable, unreadable, or indecipherable through technologies or methodologies recognized by appropriate professional organizations or standards setting bodies to provide effective security for the information) that should be applied to:
    - Vendors of PHRs;
    - Entities that offer products or services through the website of a vendor of PHRs;
    - Entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals PHRs;
    - Entities that are not covered entities and that access information in a PHR or send information to a PHR; and
    - Third party service providers used by a vendor or entity described in the above situation to assist in provided PHRs, or services;
  - A determination of which federal government agency is best equipped to enforce the requirements recommended to be applied to the vendors, entities, and services noted above: and
  - A timeframe for implementing regulations based on the findings.

- **Guidance on Implementation Specification to De-Identify PHI** – within 12 months of enactment the Secretary must, in consultation with stakeholders, issue guidance on how best to implement the requirements for the de-identification of PHI as covered in HIPAA 164.514 - Other Requirements Relating to Uses and Disclosures of PHI – Requirements for De-identification of PHI.

- **Report on Treatment Disclosures** – within 12 months of enactment the Comptroller General of the US (GAO) must summit to HELP, W&M, and E&C a report on the best practices related to the disclosure among healthcare providers of PHI of an individual for purposes of treatment of the individual. This report must include an examination of the best practices implemented by states and by other entities, such as HIEs and RHIOs, an examination of the extent to which such best practices are successful with respect to the quality of the resulting healthcare provided to the individual and with respect to the ability of the healthcare provider to manage such best practices, and an examination of the use of electronic informed consent for disclosing protected health information for treatment, payment, and health care operations.

- **Report on ARRA Impact Required** – within 5 years of enactment the GAO must submit to Congress and the Secretary a report on the impact of any of the provisions of the ARRA on health insurance premiums, overall healthcare costs, adoption of EHRs by providers and reduction in medical errors and other quality improvements.

- **Study on "Psychotherapy Notes"** – the Secretary is instructed to study the definition of "psychotherapy notes" as provided in HIPAA 164.501—Privacy Definitions. The study is to be with regard to including test data that is related to direct responses, scores, items, forms, protocols, manuals, or other materials that are part of a mental health evaluation, as determined by the mental health professional providing treatments or evaluation in such definitions and may, based on such study, issue regulations to revise such definition.

Attachment A – Privacy Sections in Order of Appearance in ARRA

Page	Section	Topic
112	Title XIII- Health Information Technology	
114-115	3000 - Definitions	Definitions that apply or reference to HIPAA definitions that apply.
117	3001 - ONC	(3) Strategic Plan (A) General (iii and ii) ONC's inclusion of privacy and security in the strategic plan.
119	3001 – ONC	(e) Establishment of the Chief Privacy Officer
120	3002 – HIT Policy Committee	(B) (i) Consideration of technologies that protect privacy and promote security
121	3002 – HIT Policy Committee	(B) (vi) Technology related to individually identifiable health information and (vii) collection of race, ethnicity, and similar data
122	3002 – Committee Membership	(2) (iv) member expertise in privacy and security
123	3002 – Outside Involvement	(5) expertise in privacy and security
125	3003 – HIT Standards Committee	(2) member expertise in privacy and security and (3) outside expertise in privacy and security
128	3009 – Relationship to HIPAA	Relationship to HIPAA privacy and security law and flexibility in administering provisions
144	Subtitle D - Privacy	
144- 145	13400 – Definitions	Definitions specifically related to privacy and security
146-	13401 –Security Provisions and Penalties to Business Associates of Covered Entities	Expansion of HIPAA security requirements to Business Associates and Guidance to be issued by HHS.
146-149	13402 – Notification in the Case of Breach	Identification and notification requirements for health information breach
149	13403 Education on Health Information Privacy	Establishment of regional privacy advisors and education programs
150	13404 Privacy Provisions and Penalties to Business Associates	Expansion of HIPAA privacy requirements to Business Associates
150-154	13405 – Restrictions, Accounting and Access	Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format
154-155	13406 – Conditions on certain contacts as part of health care operations	Contacts related to marketing and fundraising
155-157	13407 – Temporary breach notification requirements	Temporary breach notification requirements for vendors of PHRs and other non-HIPAA covered entities.
157	13408- Required Business Associate Contracts	Business associate contracts required for certain entities
157	13409 – Wrongful Disclosures	Clarification of Application of wrongful disclosures criminal penalties
157-162	Improved enforcement	Further or increased enforcement provisions and penalties

Page	Section	Topic
162	13411-Audits	Periodic audits
162-165	Part 2 – Relationship to other laws; regulatory references; effective date; and reports	
162	13421- Relationship to other laws	Relationship to state laws and HIPAA
162	13422- Regulatory References	Reference to Code of Federal Regulations
162	13423- Effective Date	Reference to Dates
162-165	13424- Studies, Reports, Guidance	Reports on compliance, application, guidance, treatment disclosures, etc., by HHS and the Government Accountability Office

Attachment B – Initial Time Tables for ARRA Sections Affecting Privacy and Security

Section	Description	Responsible Party	Due Date	Effective Date
13423	Effective date for all provisions other than those listed below.	ARRA		Except as otherwise specifically provided the provision of Sections 3000 to 13411 take effect on the data that is 12 months after the date of the enactment of this title – February 17, 2010
3001	Request for additional funding, authority, legislation, etc., including privacy and security	ONC Coordinator	Within 12 months of Enactment	
3001	Report on "lessons learned"	ONC Coordinator	Within 12 months of Enactment	
3001	Assessment of the impact of HIT on communities	ONC Coordinator	N/A	
3001	Assessment of the benefits and costs of electronic use	ONC Coordinator	N/A	
3001	Report on resources required to achieve EHR goal	ONC Coordinator	Annually	
3001	Appointment of a Chief Privacy Officer	ONC Coordinator	Within 12 months of Enactment	
3002	Appointment of HIT Policy Committee	Congress, Comptroller General , and HHS Secretary	Within 45 days from Enactment	
3004	Schedule for assessment of policy recommendations	HIT Standards Committee	Within 90 days from Enactment	
3004	Adoption, via rule making, to adopt an initial set of standards provided for under ARRA	HHS Secretary	December 31, 2009	
13401	Guidance on most effective and appropriate technologies for security	HHS Secretary	Within 12 months of Enactment	
13402	Guidance specifying the technologies and methodologies to render PHI unusable, etc.	HHS Secretary	Within 60 days of Enactment	

Section	Description	Responsible Party	Due Date	Effective Date
13402	Breach report to Congress	HHS Secretary	Within 12 months of Enactment	
13402	Interim final rules on Breach requirements for HIPAA entities	HHS Secretary	Within 180 day of Enactment	Breaches discovered 30 days or after from Interim final rule publication
13403	Designate regional office individual to provide guidance and education on privacy and security	HHS Secretary	Within 6 months of Enactment	
13403	Develop (and maintain) multi-faceted education initiative to enhance public transparency regarding uses of PHI, etc.	HHS Secretary	Within 12 months of Enactment	
13405	Limited Data Set to be consider for use by CE until Guidance on "minimum necessary" is issued	HHS Secretary		12 months of Enactment, Sunsets with effective date of HHS Guidance
13405	Guidance what constitutes "minimum necessary"	HHS Secretary	Within 18 months of Enactment	Effective date to be set by HHS
13405	Promulgate regulation on data to be provided for accounting related to EHRs	HHS Secretary	6 months after Secretary adopts standards on accounting for disclosure	Effective date varies on acquisition of EHR see 13405 (c) (4)
13405	Promulgate regulations related to prohibition on sale of EHRs or PHI.	HHS Secretary	Within 18 months of Enactment	6 months after promulgation of regulation
13406	Marketing - "reasonable in amount definition"	HHS Secretary		On or after 12 months of Enactment
13406	"Opt-Out" of Fundraising	HHS Secretary		On or after 12 months of Enactment
13407	Interim final rule related to breaches by vendors of PHRs and other non-HIPAA covered entities	FTC	Within 180 days of Enactment	Applies to breach discovery occurring on or after 30 day from interim final rule promulgation
13410	"Willful neglect" related to noncompliance			Applies to penalties imposed on or after 24 months of Enactment
13410	Rules to implement "willful neglect" penalties	HHS Secretary	Within 18 months of Enactment	Applies to penalties imposed on or after 24 months of Enactment
13410	Report on Distribution of Penalties	GAO	Within 18 months of Enactment	

Section	Description	Responsible Party	Due Date	Effective Date
13410	Regulation related to Revised Distribution of Penalties	HHS	Between 18 months and 3 years of Enactment	CMPs or Settlements imposed on or after effective date of regulation
13410	Tiered increase in amount of Civil Monetary Penalties			Amendments apply to violations occurring after the date of enactment
13410	Enforcement by State Attorneys General			Amendments apply to violations occurring after the date of enactment
13424	Report on Compliance with ARRA and HIPAA to Congress	HHS	12 Months then annually	
13424	Study and Report on application of privacy and security requirements to non-HIPAA Covered Entities to Congress	HHS Secretary in consultation with FTC	12 Months from enactment	
13424	Guidance on implementation specification to De-Identify PHI	HHS Secretary	12 Months from enactment	
13424	ARRA impact on health insurance premiums, overall health care costs, adoption of EHR by providers and reduction in medical errors and other quality improvements	HHS Secretary	Within 5 years of enactment.	