United Actuarial Services, Inc.
Actuaries and Consultants

2009-47

August 7, 2009

RESEARCH MEMO

Changes to HIPAA Privacy and Security Rules Made by New Stimulus Law

As part of the *American Recovery and Reinvestment Act of 2009 (ARRA*), changes were made to the *HIPAA Privacy* and *Security* laws. ***Most* of these changes are effective February 17, 2010 or later**.

A specially prepared copy of this Section of ARRA with a detailed table of contents for ease of use is available by "*clicking here*." This *Research Memo* is lengthy, as is the law. It concludes with a list of implementation suggestions on the last page.

At first look, some of the changes made by the new law do not jump right out. For example, the law makes certain aspects of the *HIPAA Security Rule* applicable to Business Associates. Many Business Associates already operate as if they are a covered entity under the *HIPAA Privacy* and *Security Rules* out of prudence or contractual obligation. However, the new law removes any doubts as to the applicability of the *Security Rule* requirements to Business Associates. The law makes Sections 164.308 (*Administrative safeguards*), 164.310 (*Physical safeguards*), 164.312 (*Technical safeguards*) and 164.316 (*Policies and procedures and documentation requirements*) of Title 45 of the Code of Federal Regulations applicable to Business Associates.

However, certain notice requirements in the event of a *Breach* of unsecured (unencrypted) Protected Health Information (PHI) will take effect sometime this fall. These *Breach* notice requirements are discussed in more detail later in this *Research Memo.*

In broad brush strokes, some of the biggest changes made by the law include:

- The *Security Rules* will be applicable to a Business Associate of a Health Plan in the same manner that such Sections apply to Health Plans *beginning February 17, 2010.*

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: mewing@unitedactuarial.com

- Health Plans and Business Associates have mandatory disclosure duties in the event of a *Breach* of **unsecured** PHI beginning 30 days after interim final guidance is released, which is expected to be released in August 2009.

- Health Plans will be required to comply with restrictions on the disclosure of PHI when restrictions are requested by an individual *beginning February 17, 2010;* whereas before Health Plans had an option of complying.

- Individuals will have a right to an accounting of disclosures involving *Electronic Health Records beginning in 2012 or 2014,* depending on the rule.

- Individuals will have a right to electronically access the PHI in their electronic health record if the Health Plan uses *Electronic Health Record* beginning on *February 17, 2010.*

- The Secretary of the Department of Health and Human Services (HHS) will undertake **periodic audits of Health Plans** to ensure that Health Plans and Business Associates that are subject to the expanded requirements comply with such requirements beginning on *February 17, 2010.*

Although the law applies to all "covered entities" (health plans, health care clearinghouses and health care providers), for simplicity's sake we will just refer to "Health Plans" in this *Research Memo*, except that where the term "covered entity" is used in a Section title, we will retain that term.

For original source information, See *ARRA*, *Division A-Appropriations Provisions Title XIII-Health Information Technology, Part 2-Application And Use Of Adopted Health Information Technology Standards; Reports* at Subtitle D *Privacy* (Subtitle D).

- A copy of *ARRA* is available by "*clicking here*". Title XIII begins on page 112, subtitle D begins on page 144.
- A copy of Subtitle D with a detailed table of contents for ease of use is available by "*clicking here*."
- A copy of the CRS summary on Title XIII is available by "*clicking here*"; the House Conference report at *http://thomas.loc.gov/cgi-bin/query/R?r111:FLD001:H01308* scroll down to Page: H1337.

As noted, generally, most of the changes are effective February 17, 2010. Most of the pertinent changes and effective dates were summarized above, but we'll point out the earlier and later effective dates as we discuss each Section of the law. The most important change with an earlier effective date is the mandatory duty to report a *Breach* of "unsecured PHI." "Unsecured PHI" means PHI that is not secured through the use of an encryption technology or methodology specified by HHS guidance, as discussed on pages 6-7.

A DETAILED LOOK AT THE PRIVACY/SECURITY SECTIONS

This portion of *ARRA* is found in Sections 13400-13411.

Section 13400: Definitions

This Section defines eighteen terms. Most of the definitions refer to how the term is defined in the *Privacy* or *Security* regulations. Of particular importance are three terms: *Breach, Electronic Health Record and Personal Health Record.* This *Definitions* Section can be accessed by "*clicking here*."

Essentially, a *Breach* is the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information. The full definition of *Breach* should be reviewed for the limited exceptions for "*unintentional acquisition*" and "*inadvertent disclosure*." The definition of *Breach* is important because a *Breach* of unsecure (unencrypted) PHI triggers certain notice duties by the Health Plan and/or a Business Associate.

An *Electronic Health Record* is an electronic record of health-related information on an individual that is *created, gathered, managed, and consulted* by authorized health care clinicians and staff. It is more of a thing of the future than something in widespread use and fits within the overall goal to make the whole healthcare delivery system electronic.

A *Personal Health Record* is an electronic record of identifiable health information on an individual that can be *drawn from multiple sources* and that is managed, shared, and controlled by or primarily for the individual. It too is more of a thing of the future than something in widespread use.

Section 13401: Application Of Security Provisions And Penalties To Business Associates Of Covered Entities; Annual Guidance On Security Provisions

This Section makes the *Security Rules* concerning *administrative safeguards*, *physical safeguards*, *technical safeguards* and *policies, procedures and documentation requirements* **applicable to a Business Associate** of a Health Plan in the **same manner** *that such Sections apply to Health Plans. This change is effective beginning February 17, 2010.* Since, out of prudence, many Business Associates already conduct operations as if the *Security Rules* applied to them directly, in addition to the duties imposed by their Business Associate contracts, this change may not make much practical difference in operation. There is a new requirement that this application of the *Security Rules* to *Business Associates* be incorporated into the Business Associate agreement between the Business Associate and the Health Plan. This change will provide an opportunity for Health Plans and their Business Associates to review the Rules and their internal

operations. It is safe to assume that these new requirements will probably give rise to the need for Health Plans and Business Associates to execute addendums or new contracts.

In addition, the law makes the civil and criminal penalties for breaching the Rules applicable to *Business Associates* just as they are currently imposed on Health Plans for violations of the Rules.

This Section calls for the HHS to issue guidance annually on the most effective and appropriate technical safeguards for use in carrying out the *Security Rule* Sections in Subtitle D, as well as other privacy and security standards.

See the Research Department's *Topical Index* at page 9 under the section on ***Privacy and Security Rules Under HIPAA*** for Research Department publications on the *Security Rule.* The *Topical Index* can be accessed at: *http://www.unitedactuarial.com/research/docs/topical_index/topind_pdflinks.pdf.*

Detailed information on the *Security Rule* can also be found on the HHS website at: *http://www.cms.hhs.gov/SecurityStandard/.*

Section 13402: Notification In The Case Of Breach

This Section details the requirements for Health Plans to give notice to individuals of *Breaches* of **unsecured** PHI and also sets out the requirements for Business Associates to notify a Health Plan if any *Breaches* of unsecured PHI occur. "*Click here*" for a list of the Notice requirements in the event of a Breach of unsecured PHI.

The Notice requirements are quite detailed and may provide impetus for Health Plans to investigate the costs of securing (encrypting) PHI. The Notice requirements apply only to *Breaches* of unsecured PHI. The theory apparently being "secure" PHI cannot be breached and no notice is therefore required. However, there may be state laws applicable to breach of some of the personal identifiers that can make up PHI, especially Social Security Numbers. See *Research Memo 2008-25* and *http://www.ncsl.org/Default.aspx?TabId=13489.*

As mentioned previously, "**unsecured PHI**" means PHI that is not secured through the use of an encryption technology or methodology specified by HHS guidance. As discussed below, HHS has issued preliminary guidance on securing PHI.

Even if your Health Plan has not experienced a *Breach* of unsecured PHI, it may be advisable to investigate the encryption technology discussed in the preliminary guidance on the subject, discussed below. The trend in data security seems to be moving toward encryption, so even if implementation of this technology is not in a Health Plan's immediate future it would be advisable to consider this technology at some point. If a Health Plan does not decide to encrypt its PHI, the Health Plan should prepare notice forms for use in the event of a *Breach*.

In this somewhat lengthy Section, we'll take a detailed look at the Notice content and timing requirements for giving notice of a *Breach* of unsecured PHI.

Who Must Give Notice of a Breach of Unsecured PHI?

If the Health Plan discovers a *Breach* of unsecured PHI, the Health Plan must ***notify each individual*** whose information has been, or is reasonably believed by the Health Plan to have been, accessed, acquired or disclosed as a result of such *Breach.*

A Notice requirement also applies to any Business Associate of a Health Plan. If the Business Associate discovers a *Breach* of unsecured PHI, the Business Associate must ***notify the Health Plan*** of the *Breach*. The Notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such *Breach.* The Health Plan then is the entity responsible for notifying the individual in the event a *Breach* is detected by the Business Associate.

HHS Issued Preliminary Guidance on "Securing" PHI

HHS issued preliminary guidance and a request for information, available by "*clicking here*." The guidance does not apply to any *Breaches* until 30 days after publication of interim final regulations. The preliminary guidance identifies the technologies and methodologies that can be used to render PHI unusable, unreadable or indecipherable to unauthorized individuals. The guidance should be used by Health Plans and their Business Associates to determine whether ''unsecured PHI'' has been *Breached*, which triggers the notification requirements of Section 13402. Persons responsible for PHI Security at Health Plans and Business Associates should read this brief (5 pages) preliminary guidance. It is not discussed in detail herein.

According to the guidance, HHS has identified two methods for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals: (1) *encryption* and (2) *destruction.* Approved methods of encryption are discussed at pages 4 and 5.

The two encryption processes that have been tested by the National Institute of Standards and Technology (NIST) and judged by HHS to meet the law's requirements are:

(1) Valid encryption processes for data at rest that are consistent with NIST Special Publication 800–111, *Guide to Storage Encryption Technologies for End User Devices*; and

(2) Valid encryption processes for data in motion that comply with the requirements of Federal Information Processing Standards (FIPS) 140–2. These include, as appropriate, standards described in NIST Special Publications 800–52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800–77, *Guide to IPsec VPNs*; or 800–113, *Guide to SSL VPNs*, and may include others which are FIPS 140–2 validated.

The NIST publications are available from the NIST website at: *http://www.csrc.nist.gov/publications/PubsSPs.html*. The FIPS document is available at: *http://www.csrc.nist.gov/publications/PubsFIPS.html.*

When Must Notice of a Breach of Unsecured PHI Be Given?

A Health Plan or a Business Associate shall be treated as discovering the *Breach* on the first day the *Breach* is known or should have been known to the Health Plan or Business Associate. Once the *Breach* is discovered, the law has specific rules about when to notify individuals, and/or the media and/or HHS. Health plans will need to keep logs of any such *Breaches* and document the notification activity taken.

Generally, **all notifications** shall be **made *without unreasonable delay* but no later than *60 calendar days* after the discovery of a *Breach*** by the Health Plan or Business Associate involved.

What Records of Giving Notice Of Such Breach Must Be Kept?

The Health Plan or Business Associate involved in a required notification will have the burden of demonstrating that all notifications were made as required, including evidence demonstrating the necessity of any delay. Health Plans or Business Associates should plan ahead to keep true, accurate and easily accessible records of sending such notices.

What Are the Acceptable Methods Of Giving Notice of Such A Breach?

Since Business Associates only have to notify the Health Plan, this discussion focuses on the Notice that Health Plans would provide to the individuals. The law provides rules for sending required Notices to individuals, as well as ways of providing Notice through mass media and the internet, depending on the number of individuals affected. Health Plans should begin preparing model Notices that contain the required data elements so the will be ready in the event of a *Breach* of unsecured PHI. The content of the Notice of *Breach* is discussed below.

What is the Required Content For A Notice Regarding the Breach of Unsecured PHI?

A Notice for a *Breach* of unsecured PHI must include, to the extent possible, the following:

- A brief description of what happened, including the date of the *Breach* and the date of the 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 Health Plan 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 must include a toll-free telephone number, email address, Website or postal address.

Effective Date of Notice For the Breach of Unsecured PHI Regulations

HHS is expected to publish interim final regulations sometime in late August 2009. The provisions of this Section apply to *Breaches* that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations. Thus, the notice requirement for the *Breach* of unsecured PHI would probably apply in Fall 2009. There is no requirement to encrypt PHI.

Section 13403: Education On Health Information Privacy

This Section addresses educational efforts about health information privacy to be made by HHS. The interested reader can read the Section on their own.

Section 13404: Application Of Privacy Provisions And Penalties To Business Associates Of Covered Entities

This Section makes *HIPAA Privacy* and *Security Rules* applicable to Business Associates, including any civil or criminal penalties. These penalties are discussed in detail below in Section 13410.

Section 13405: Restrictions On Certain Disclosures And Sales Of Health Information; Accounting Of Certain Protected Health Information Disclosures; Access To Certain Information In Electronic Format

This Section addresses various new restrictions on the use and disclosure of PHI.

Requested Restrictions on Certain Disclosures of Health Information

If an individual requests that a Health Plan restrict the disclosure of the individual's PHI, the Health Plan must comply with the requested restriction if –

(1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and

(2) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid in full by the individual.

Previously, the Health Plan could determine whether to comply with such a request.

Disclosures Required to Be Limited to the Limited Data Set or the Minimum Necessary

A Health Plan shall be treated as being in compliance with respect to the use, disclosure or request of PHI only if the Health Plan limits such PHI, to the extent practicable, to the "limited data set" or, if needed by the Health Plan, to the "minimum necessary" to accomplish the intended purpose of such use, disclosure or request. In choosing such information, the Health Plan or Business Associate shall determine what constitutes the "minimum necessary" to accomplish the intended purpose of such disclosure until guidance is issued. "*Click here"* for a definition of a "limited data set."

Guidance on what constitutes "minimum necessary" is expected to be issued in **August 2010.** The guidance shall take into consideration the information necessary to improve patient outcomes and to detect, prevent and manage chronic disease.

Accounting of Certain PHI Disclosures Required if Covered Entity Uses Electronic Health Record

An individual shall have a right to receive an accounting of disclosures *made by a Health Plan that uses or maintains an Electronic Health Record* with respect to PHI during the three years prior to the date on which the accounting is requested. The use of an *Electronic Health Record* is not required.

Regulations on what information should be collected about each disclosure will be published by the HHS not later than six months after the date on which HHS adopts standards on accounting for disclosure. These regulations will only require that information be collected through an *electronic health record* in a manner that takes into account the interests of the individuals in learning the circumstances under which their PHI is being disclosed and *takes into account the administrative burden of accounting for such disclosures.*

The effective dates for these disclosures range from January 1, 2011 to January 1, 2014 and possibly later. "*Click here*" for more detailed information relating to this subsection (c) of Section 13405.

If a Health Plan uses or maintains an *Electronic Health Record* with respect to PHI of an individual, the individual will have a right to obtain from such Health Plan a copy of such information in an electronic format and, if the individual chooses, to direct the Health Plan to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous and specific. The use of an *Electronic Health Record* is NOT required.

Any fee that the Health Plan may impose for providing such individual with a copy of such information (or a summary or explanation of such information), if such copy (or summary or explanation) is in an electronic form, shall not be greater than the Health Plan's labor costs in responding to the request for the copy (or summary or explanation).

Section 13406: Conditions On Certain Contacts As Part Of Health Care Operations

This Section addresses rules on marketing by Health Plans or Business Associates to plan recipients, payments associated with such marketing and fund-raising opt-outs. "Marketing" is generally "a communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service. Whether the activity falls within an allowable exception is found in more detail in this Section of the law. With limited exceptions, the *Privacy Rule* requires an individual's written authorization before a use or disclosure of his or her PHI can be made for marketing. So as not to interfere with core health care functions, the *Privacy Rule* distinguishes marketing communications from those communications about goods and services that are essential for quality health care.

Frequently Asked Questions on Marketing can be found at the Office of Civil Rights website:

- Marketing Definition
  http://www.hhs.gov/ocr/privacy/hipaa/faq/use/index.html#MarketingDef

- Marketing Uses
  http://www.hhs.gov/ocr/privacy/hipaa/faq/use/index.html#Uses

- Individual Protections
  http://www.hhs.gov/ocr/privacy/hipaa/faq/use/index.html#Protections

The effective date of this Section is February 17, 2010.

Section 13407: Temporary Breach Notification Requirement For Vendors Of Personal Health Records And Other Non-HIPAA Covered Entities

This Section applies to **vendors of personal health records** (PHR) that discover a *Breach* of security of unsecured PHR identifiable health information that is in a *Personal Health Record* maintained or offered by such vendor. There are a number of details that address the *Application of Requirements for Timeliness, Method and Content of Notifications*, *Notification of the Federal Trade Commission*; *Enforcement* as an unfair and deceptive act or practice in violation of the Federal Trade Commission Act. The interested reader can read the Section on their own.

Section 13408: Business Associate Contracts Required For Certain Entities

This Section requires a written contract (or *other written arrangement*) as described in the *Privacy* and *Security Rules* at 45 CFR Section 164.502(e)(2); and 45 CFR Section 164.308(b) for each organization that:

- provides data transmission of PHI to a Health Plan or its Business Associate
- requires access on a routine basis to such PHI, such as a *Health Information Exchange Organization*, *Regional Health Information Organization*, *E-prescribing Gateway*, or
- contracts with a Health Plan to allow that Health Plan to offer a personal health record to patients as part of its electronic health record, Such organizations will be treated as a Business Associate of the Health Plan.

Section 13409: Clarification Of Application Of Wrongful Disclosures Criminal Penalties

This Section clarifies that criminal penalties for wrongful disclosure of PHI or other protected information apply only if the individual obtained or disclosed such information without authorization.

Section 13410: Improved Enforcement

This Section states a violation of a provision of *ARRA* that is due to willful neglect is a violation for which HHS is required to impose a penalty. HHS will formally investigate any complaint of a violation of a provision of this part of *ARRA* if a preliminary investigation of the facts of the complaint indicates a possible violation due to "willful neglect." Civil money penalties range from:

- $100 per violation, not to exceed $25,000 per year for the same type of violation;
- $1,000 per violation if due to reasonable cause and not willful neglect, with a $100,000 cap; and
- $10,000-$50,000 in instances of willful neglect, with a $250,000 to $1.5 million cap.

There are also criminal penalties associated with *Privacy/Security Rule* violations that apply to knowingly and improperly disclosing or obtaining PHI under false pretenses. Criminal penalties range from:

- $50,000 and one year in prison for intentionally obtaining or disclosing PHI;
- up to $100,000 and up to five years in prison for obtaining PHI under "false pretenses"; and
- up to $250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Section 13411: Audits

This Section states that HHS will provide for **periodic audits** to ensure that Health Plans and Business Associates that are subject to the requirements of this Part D comply with such requirements.

COMPLIANCE SUGGESTIONS

Here are a few compliance suggestions for Trustees, administrators and plan professionals to consider in light of the general February 17, 2010 compliance date:

- Health Plans should consider contacting their Business Associates to notify them of the changes to these laws.

- Health Plans will need to determine if they are going to secure (encrypt) their PHI. This will take some time to decide and more time to implement if encryption is chosen. In the interim, Health Plans should develop forms for disclosing *Breaches* of unsecured PHI, if any, as set out in the law.

- Health Plans should work with their IT Department to investigate the pros and cons of adopting encryption technology or methodology that meets HHS preliminary guidance.

- Health Plans will need to update their *HIPAA Privacy and Security Manuals* to reflect the changes made by the law and train their staff accordingly.

- Health Plans will need to make changes in their standard Business Associate contracts to reflect the changes made by the law.

- Health Plans will probably need to update their *Notice of Privacy Practices* to reflect the changes made by the law and distribute the Revised Notice.

- Health Plans should review their use of PHI to make sure such uses comply with the new Sections on such uses.

- Health Plans should develop a plan of action and timeline for implementing these required changes.

- Discuss these changes with the Board of Trustees.

Until additional guidance issued, the only guidance is a reasonable interpretation of the statute. There will probably be a flurry of guidance issued much like when the original *Privacy Rule* was promulgated. We will report on additional guidance as it is issued.

* * *