United Actuarial Services, Inc.
Actuaries and Consultants

2013-09

February 12, 2013

CLIENT BULLETIN

New HIPAA Rules Affect Plans, Business Associates, Subcontractors, Breach of PHI Standard and More!!!

The Department of Health and Human Services (HHS or "the Department") recently published a *Final Rule* ("regulations") in the *Federal Register* (78 FR 5566) with a name that's a mouthful:

> *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules*

- **The *Final Rule* is effective on March 26, 2013.**
- **However, *Covered Entities* and *Business Associates* generally have until September 23, 2013 to be *compliant*.**
- **A delayed *compliance* date of September 23, 2014 also generally applies to the required changes to *Business Associate Agreements*.**

As the *Rule's* name implies, the *Final Rule* is intended to:

- modify the *Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules* to implement statutory amendments under the *Health Information Technology for Economic and Clinical Health Act* ("*the HITECH Act" or "the Act*") to strengthen the privacy and security protection for individuals' health information;
- modify the rule for *Breach Notification for Unsecured Protected Health Information* (*Breach Notification Rule*) under the *HITECH Act*;
- modify the *HIPAA Privacy Rule* to strengthen the privacy protections for genetic information under the *Genetic Information Nondiscrimination Act of 2008 (GINA)*; and
- make certain other modifications to the *HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules).*

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

The *Rule* is referred to as an Omnibus Rule as it is comprised of four separate final rules. The full *Federal Register* document runs 138 pages, with the regulations section 16 pages long. As a study aid, we have added references to page numbers in the *Preamble* of various topics in the *Rule* disused herein.

Changes Made By These New Rules

There are several big changes made by the *Final Rule* compared to the prior *HIPAA Rules.* One of these is the change of the definition of "breach" and of the standard used in determining whether there has been a "breach" and "unauthorized disclosure" of *Protected Health Information (PHI)."* The rule also makes Business Associates (which now includes "subcontractors") directly liable under Sections of the *HIPAA Rules.* These and other changes are discussed in detail below. In future issues we will focus on some of these major changes in greater detail.

HHS notes that going forward, Covered Entities will always have a 180-day delayed compliance date from any new rule's effective date, as applies to these rules, as noted in the text box on page 1 of this *Client Bulletin*.

Major changes affect:

- Business Associates [78 FR 5570-74, 5597, 98],
- Business Associate Agreements [78 FR 5599-5602],
- Subcontractors to Business Associates [78 FR 5572, 73],
- Subcontractor Agreements [78 FR 5599-5602],
- Breach and Notification Rules [78 FR 5639-47, 5647-55],
- Notice of Privacy Practices [78 FR 5622-26],
- Right of an individual to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full [78 FR 5626-30].

Changes of less relevance to multiemployer health plans include:
For information on these items see pages listed or "linked" documents.

- Strengthening the limitations on the use and disclosure of PHI for *marketing* [78 FR 5592] and *fundraising* [78 FR 5618-22] purposes, and prohibiting the *sale* [78 FR 5603-08] of PHI without individual authorization.
- Expanding individuals' *rights to receive electronic copies of their health information* [78 FR 5631-38].
- Modifying the individual authorization and other requirements to facilitate research and *disclosure of child immunization proof to schools*, and to enable *access to decedent information* by family members or others [78 FR 5616-18].
- Adopting the additional *HITECH Act* enhancements to the *Enforcement Rule* not previously adopted in the October 30, 2009 interim final rule such as the *provisions addressing enforcement of noncompliance* with the *HIPAA Rules* due to willful neglect [78 FR 5578-79].

- Adopting changes to the *HIPAA Enforcement Rule* to incorporate the *increased and tiered civil money penalty structure* provided by the *HITECH Act* [78 FR 5579-87].
- Adopting changes modifying the *HIPAA Privacy Rule* as required by the *Genetic Information Nondiscrimination Act (GINA)* to prohibit most health plans from *using or disclosing genetic information for underwriting purposes* [78 FR 5658-64].

> The prior interim rules and laws were discussed in *Research Memo 2009-47*, *Special Bulletin 2009-50*, *Special Bulletin 2010-14*, *Benefit News Briefs 2010-23*, and *Benefit News Briefs 2010-54*.

In this *Client Bulletin* we specifically look at:

- the change in the definition of "breach";
- the new analysis used to determine if a "breach" of privacy has occurred;
- the "notice of breach" rules;
- application of the *HIPAA Privacy* and *Security Rules* to Business Associates, Subcontractors; and
- Business Associate Agreement Rules and HHS sample language; and
- some miscellaneous changes.

The New Definition of "Breach" and "Breach" Analysis

The regulation adds language to the definition of "breach" of the *Privacy Rules* to clarify that an "*impermissible use or disclosure*" of *PHI* is ***presumed*** to be a breach *unless* the Covered Entity or Business Associate demonstrates that there is a *low probability* that the PHI has been *compromised* based on a risk assessment. "*Covered Entities" are: (1)* health care providers who conduct covered health care transactions electronically, (2) health plans, and (3) health care clearinghouses. Since our audience is primarily multiemployer health care plans, for this *Client Bulletin*, we will use the term "health care plan" instead of "Covered Entity".

This is a major change in the standard and analysis of whether such a "disclosure" was a "breach". The heart of the *prior definition* of "breach" was:

> A "breach" is, generally, an impermissible use or disclosure under the Privacy Rule that *compromises the security or privacy* of the protected health information such that the use or disclosure *poses a significant risk of financial, reputational, or other harm* to the affected individual.
>
> *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html*

Thus, the old standard focused on a "*significant risk of financial, reputational, or other harm*" before an impermissible use or disclosure was a "breach."

Now, instead of a "*harm*" standard to determine if a "breach" occurred, the health care plan or Business Associate must determine if there is a "*low probability*" that the PHI has been *compromised* based on a *risk assessment* that considers at least the following four factors:

(1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(2) the unauthorized person who used the PHI or to whom the disclosure was made;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk to the PHI has been mitigated.

The *Preamble* notes that "*Other factors may also be considered where necessary*." HHS further states that in the future it will "issue additional guidance to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios."

Health care plans or Business Associates should document any such "disclosures" and subsequent "risk assessment," including the analysis and considering the above factors. Failure to do so could prove expen$ive.

Notice of Breach

If there is not a low probability the *PHI* has been compromised, then certain "notice" rules apply to health care plans and Business Associates. [78 FR 5638].

Health care plans should specify the duties regarding breach notification of Business Associates, including subcontractors, in their Business Associate contracts. The *Final Rule* makes clear that a health care plan is not required to enter into a contract or other arrangement with a Business Associate that is a subcontractor. It is the Business Associate that must obtain the required satisfactory assurances from the subcontractor to protect the security of electronic *PHI.*

The *HITECH Act* requires *HIPAA* health care plans to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured PHI. In some cases, the *Act* also requires health care plans to provide notification to the media of breaches. In the case of a breach of unsecured PHI at or by a Business Associate of a health care plan, the *Act* requires the Business Associate to notify the health care plan of the breach. Finally, the *Act* requires the Secretary to post a list of health care plans that experience breaches of unsecured PHI involving more than 500 individuals on an HHS website.

Business Associates and Subcontractors

The new *Rules* make Business Associates of health care plans directly liable for compliance with certain *HIPAA Privacy and Security Rules* requirements.

The term "Business Associate" is defined to include a "*subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate*."

A "subcontractor" is a person to whom a Business Associate has delegated a function, activity, or service that the business associate has agreed to perform for a health care plan or Business Associate. If a subcontractor contracts with another entity to assist in its duties, that subcontractor also becomes a Business Associate and liable under the *HIPAA Rules* in the same manner as the primary Business Associate and so on down the line.

In particular, Business Associates must comply with the *Security Rule's* administrative, physical, technical, and organizational safeguard requirements in Sections 164.308, 164.310, 164.312 and 164.314, as well as the *Security Rule's* policies, procedures and documentation requirements in Section 164.316 in the same manner as these requirements apply to health care plans. Business Associates are civilly and criminally liable for violations of these provisions.

According to the *Preamble*: Business Associates (including subcontractors) are directly liable under the *HIPAA Rules* for:

- impermissible uses and disclosures;
- for a failure to provide breach notification to the health care plan;
- for a failure to provide access to a copy of electronic PHI to either the health care plan, the individual, or the individual's designee (whichever is specified in the Business Associate Agreement);
- for a failure to disclose PHI where required by the Secretary to investigate or determine the business associate's compliance with the *HIPAA Rules;*
- for a failure to provide an accounting of disclosures, or
- a failure to comply with the requirements of the *Security Rule*.

Business Associates remain contractually liable for other requirements of the Business Associate Agreement in addition to the above liabilities.

Business Associate Agreements [78 FR 5599-5602]

The *Rule* makes some changes to what must be included in a Business Associate Agreement. The *Final Rule* makes it clear that a health care plan is not required to enter into a contract or other arrangement with a Business Associate that is a subcontractor. It is the Business Associate that must obtain the required satisfactory assurances from the subcontractor to protect the security of PHI.

HHS refers Business Associates to the HHS educational papers and other compliance guidance with the *HIPAA Security Rule* found at: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule*. These materials

provide guidance on conducting risk analysis and implementing the other administrative safeguards required by the *Security Rule*, which may prove helpful to Business Associates while they facilitate their compliance efforts.

Transition Business Associate Agreement Rules [78 FR 5602-5603]

The new *Rule* allows a *transition period* to allow health care plans and Business Associates (and Business Associate Subcontractors) to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the *Rules*, that is until September 23, 2014.

The additional transition period would be available to a health care plan or Business Associate **if,** prior to January 25, 2013, the health care plan or Business Associate had an existing contract or other written arrangement with a Business Associate or Subcontractor, respectively, that complied with the prior provisions of the *HIPAA Rules* and such contract or arrangement was not renewed or modified between March 26, 2013 and September 23, 2013. Otherwise, any modifications or renewals between such dates would require the Business Associate Agreement to comply with the new *Rules.*

According to the *Preamble*, the proposed provisions were intended to allow those health care plans and Business Associates with valid contracts with Business Associates and Subcontractors, respectively, to continue to disclose PHI to the Business Associate or Subcontractor, or to allow the Business Associate or Subcontractor to continue to create or receive PHI on behalf of the health care plan or Business Associate until September 23, 2014, regardless of whether the contract meets the requirements in the modifications to the *Rules*.

With respect to Business Associates and Subcontractors, the rules would grandfather existing written agreements between Business Associates and Subcontractors. Such contracts will be deemed to be compliant until either the health care plan or Business Associate has renewed or modified the contract after September 23, 2013 or until September 23, 2014, whichever is sooner.

With respect to those Business Associate Agreements that have already been renegotiated in good faith to meet the applicable provisions in the *HITECH Act*, health care plans should review such agreements to determine whether they meet the *Final Rule's* provisions. If they do not, these health care plans then have the transition period to make whatever additional changes are necessary to conform to the *Final Rule*.

Given the changes to the definition of "breach," it will not be surprising if most Business Associate Agreements will need to be revised as many health plans used the prior definition of "breach" in the Business Associate Agreement. Business Associate Agreements that incorporate by reference the definition of "Breach" may be able to avoid revision of that section. Though other items may need revision.
In any case, now is the time to review and revise Business Associate Agreements and Subcontractor Agreements and perform an inventory confirming the health care plan has signed contracts with each of its Business Associates in place.

HHS has released sample Business Associate Agreement materials that can be helpful in drafting/revising Business Associate/Subcontractor Agreements at: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html* or by "*clicking here.*"

The *HIPAA Security Rule* and Business Associates After *HITECH*

As noted, the *HITECH Act* provides that the *Security Rule's* administrative, physical, technical, and organizational safeguards requirements in Sections 164.308, 164.310, 164.312, and 164.314, as well as the *Rule's* policies and procedures and documentation requirements in Section 164.316, apply to Business Associates in the same manner as these requirements apply to health care plans. Business Associates are civilly and criminally liable for violations of these provisions.

The *Security Rule* currently requires a health care plan to establish a Business Associate Agreement that requires Business Associates to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that they create, receive, maintain or transmit on behalf of the health care plan as required by the *Security Rule*; and to ensure that any agent, including a Subcontractor, to whom they provide such information agrees to implement reasonable and appropriate safeguards to protect it.

Consequently, according to the *Preamble*, Business Associates and Subcontractors should already have in place security practices that either comply with the *Security Rule*, or that require only modest improvements to come into compliance with the *Security Rule* requirements.

Notice of Privacy Practices

The *Final Rule* adopts the modification which requires certain statements in the Notice of Privacy Practices (NPP) regarding uses and disclosures that require "authorization." The *Final Rule* does not require the NPP to include a list of all situations requiring authorization. The *Preamble* notes health care plans that do not record or maintain psychotherapy notes are not required to include a statement in their NPPs about the authorization requirement for uses and disclosures of psychotherapy notes.

The *Final Rule* adopts the proposed requirement for a statement in the NPP regarding fundraising communications and an individual's right to opt out of receiving such communications, **if** a health care plan intends to contact an individual to raise funds for the health care plan.

The *Final Rule* also adopts the proposal that the NPP inform individuals of their new right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service. Only health care **providers are required** to include such a statement in the NPP. Such language is **optional for health care plans**.

The *Final Rule* also requires health care plans to include a statement in their NPP of the right of affected individuals to be notified following a breach of unsecured PHI. The *Preamble* notes a simple statement in the NPP that an individual has a right to or will receive notifications of breaches of his or her unsecured PHI will suffice for purposes of this requirement.

These changes represent material changes to the NPP of covered entities.

Section 164.520(c)(1) of the *Final Rule* requires a health plan that currently posts its NPP on its web site to: (1) prominently post the material change or its revised notice on its web site by the effective date of the material change to the notice (e.g., the compliance date of this *Final Rule*) and (2) provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan, such as at the beginning of the plan year or during the open enrollment period.

Health plans that do not have customer service web sites are required to provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the material revision to the Notice. These requirements apply to all material changes including, where applicable, the rule change adopted pursuant to GINA that prohibits most health plans from using or disclosing genetic information for underwriting purposes.

To the extent that some covered entities have already revised their NPPs in response to the enactment of the *HITECH Act* or State law requirements, HHS clarified that as long as a health care plan's current NPP is consistent with this *Final Rule* and individuals have been informed of all material revisions made to the NPP, the health care plan is not required to revise and distribute another NPP upon publication of this *Final Rule*.

Health plans will want to review their NPPs and determine if they are currently compliant or if they need to be revised and redistributed.

MISCELLENEOUS

Protection Of PHI For 50 Years After Death

The new rules amend the prior rules to require a health care plan comply with the requirements of the *Privacy Rule* with regard to the PHI of a deceased individual for a period of 50 years following the date of death. The individually identifiable health information of a person who has been deceased for more than 50 years is not PHI under the *Privacy Rule*. The *Preamble* notes that the 50-year period of protection is not *a record retention requirement*. The *HIPAA Privacy Rule* does not include medical record retention requirements and health care plans may destroy such records at the time permitted by State or other applicable law.

Disclosure By Health Care Plans Of A Decedent's Information To Family Members And Others

The new *Rule* amends the prior rule to permit health care plans to disclose a decedent's information to family members and others who were involved in the care

or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual known to the health care plan.

Disclosure By Covered Entities Of School Immunization Records

Although probably more applicable to providers than health care plans, the new rules allow health care plans to disclose proof of immunization to schools in States that have school entry or similar laws.

Communicating To Individuals With Unencrypted Emails

While this change would appear to apply more to providers, it also affects health care plans to the extent they communicate with individuals via email. The *Preamble* notes that health care plans are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. HHS disagrees that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on health care plans and believes this is a necessary step in protecting PHI.

HHS does NOT expect health care plans to educate individuals about encryption technology and information security. Rather, health care plans are merely expected to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive PHI in that way, and health care plans are not responsible for unauthorized access of PHI while in transmission to the individual based on the individual's request and are not responsible for safeguarding information once delivered to the individual.

GINA

The *Final Rule* adopts the approach of the proposed rule to apply the prohibition on using or disclosing PHI that is genetic information for underwriting purposes to all health care plans.

The *Final Rule* adopts the requirement for health care plans that perform underwriting to include in their NPPs a statement that they are prohibited from using or disclosing genetic information for such purposes. Health care plans that have already modified and redistributed their NPPs to reflect the statutory prohibition are not required to do so again, provided the changes to the NPP are consistent with this rule.

Time To Start Reviewing Plan Policies, Procedures And Notices

Health care plans and plan professionals should begin reviewing Plan policies, procedures and notices in order to bring them into compliance with these *Rules.* Fortunately, the *Rules* have delayed compliance dates for these changes which should allow Plans and Plan professionals to take an orderly approach to compliance reviews. Addressing the new "low probability" standard for determining if there has been a "breach" of PHI, the Business Associate rules and Privacy Notice rules stand out as obvious areas where Plans will have some updating work to do.

* * *