Compliance Bulletin

Final Omnibus Rule

MODIFICATIONS TO HIPAA PRIVACY, SECURITY, ENFORCEMENT AND BREACH NOTIFICATION RULES

September 10, 2013

www.HealthPlansInc.com

HealthPlans, Inc.

Inside:

Overview

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) issued final omnibus regulations ("Final Rule") making modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules to implement requirements under the HITECH Act and the Genetic Information Nondiscrimination Act ("GINA"). The Final Rule was effective March 26, 2013 and "Covered Entities" and "Business Associates" must comply no later than **September 23, 2013.** The provisions of the Final Rule applicable to your group health plan ("Plan") (as a Covered Entity) and to **Health Plans** (as a Business Associate of your Plan) are set forth below.

Defining the terms

A ***COVERED ENTITY*** is a health plan, a health care clearinghouse, or a health care provider.

A ***BUSINESS ASSOCIATE*** is an entity that creates, receives, maintains or transmits PHI on behalf of the Covered Entity.

This Bulletin will also be available for download in the **Employers and Brokers** sections of our website, **www.HealthPlansInc.com**, under "Regulatory Compliance".

Business Associates – Subcontractors – Business Associate Agreements

Business Associates

Under the original 1996 HIPAA regulations, only Covered Entities were directly liable for HIPAA violations with direct enforcement by HHS. The Final Rule makes Business Associates (entities that create, receive, maintain or transmit Protected Health Information ["PHI"] on behalf of a Covered Entity) **directly liable** for compliance with the Security Rule and certain standards under the Privacy Rule as set forth in the Business Associate Agreement between the Business Associate and Covered Entity. Specifically, Business Associates are directly liable for violations of applicable HIPAA privacy, security and breach notification rules, including

- failure to comply with the Security Rule's administrative, physical and technical safeguards and documentation requirements;
- impermissible uses and disclosures of PHI;
- failure to provide an accounting of disclosures of PHI;
- failure to respond to an individual's request for a copy of electronic PHI;
- failure to provide notification to a Covered Entity of a breach of unsecured PHI;
- failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose;
- failure to comply with documentation requirements including written policies and procedures and executing Business Associate Agreements; and
- failure to disclose PHI when required by the Secretary of HHS to determine Business Associates compliance.

Business Associates are already **contractually** required to comply with the above requirements through their Business Associate Agreements. In addition, Business Associates are contractually required to perform certain other activities set forth in their Business Associate Agreements for which direct HIPAA liability does not apply.

Subcontractors

Under the Final Rule, Business Associates **include all subcontractors** of the Business Associate which create, receive, maintain or transmit PHI on behalf of the Business Associate no matter how far "downstream" the subcontractors may be. Subcontractors are entities to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of the Business Associate.

Business Associates must obtain "satisfactory assurances" from subcontractors through a Business Associate Agreement (or similar agreement) that the subcontractor will agree to the same restrictions and conditions with respect to PHI that apply in the Business Associate Agreement between the Business Associate and Covered Entity.

Covered Entities are not required to enter into a Business Associate Agreement with the Business Associate's subcontractors.

Covered Entities are now liable for Business Associate's actions if the Business Associate is considered an "agent" of the Covered Entity; and the Business Associate will be liable for its subcontractor's actions if the subcontractor is considered an "agent" of the Business Associate.

Defining the terms

AGENCY is determined under federal common law (irrespective of what the contract says) and is based on whether the Covered Entity retains authority to control the Business Associate (or for a Business Associate, whether the Business Associate retains authority to control its subcontractor).

Business Associate Agreements – Content

In addition to the content required under HIPAA and the HITECH Act, the Final Rule requires that Business Associate Agreements contain the following provisions:

- Business Associate must comply with the Security Rule and report a Security Breach to the Covered Entity.
- Business Associate must comply with the Privacy Rule as it applies to the obligations delegated to the Business Associate under the Agreement.
- Business Associate must enter into a Business Associate Agreement (or similar agreement) with subcontractors containing the same or greater protections of PHI as set forth in the Business Associate Agreement with the Covered Entity.
- Business Associate that is aware of non-compliance by a subcontractor must respond to the situation in the same manner as the Covered Entity would if the Business Associate was not compliant.
- Business Associate must agree to comply with the HITECH standards regarding marketing, genetic information, and individuals' rights to access their PHI in electronic format.
- Business Associate Agreements no longer need to include the requirement for a Covered Entity to report a Business Associate's violations of the Agreement.

The Final Rule provides a one-year transition period for existing Business Associate Agreements.

If the Agreement was in place prior to January 25, 2013 (the date the Final Rule was published in Federal Register), it complied with the prior provisions of the HIPAA Privacy and Security Rules, and it is not modified or renewed (except auto renewal) any time between March 26, 2013 and September 23, 2013, then the Agreement does not need to be modified to include the new provisions until the earlier of

i) the date the Agreement is modified or renewed; or
ii) September 23, 2014.

Marketing and Sale of Protected Health Information

Marketing

The Final Rule expands what uses and disclosures of PHI are considered "marketing" and, as such, require an individual's authorization. Authorization is required for all treatment and healthcare operations communications where the Covered Entity receives financial remuneration for making the communication from a third party whose product or service is being marketed.

- Marketing communications are "all subsidized communications that market a health-related product or service."
- Financial remuneration includes payments made in exchange for making communications about a product or service; it does not include non-financial benefits.

If a Business Associate or subcontractor receives the financial remuneration for making the communication (instead of the Covered Entity), individual authorization is needed.

The Authorization must state if financial remuneration will be paid to the Covered Entity or Business Associate.

The following communications are allowed without authorization:

- face-to face communications related to treatment or health care operations even if financial remuneration is received from a third party
- gifts of promotional or nominal value
- communications related to health in general (e.g. diet, routine diagnostic tests)
- communications related to government-sponsored programs such as Medicare or Medicaid
- communications about a drug or biologic that is currently prescribed to an individual (e.g. "re-fill reminders") as long as any financial remuneration is reasonably related to the Covered Entity's cost of making the communication

Sale of PHI

HIPAA's privacy requirements in place before the Final Rule allowed the sale of an individual's PHI for otherwise permitted uses and disclosures only if a Covered Entity received an individual's authorization. The Final Rule clarifies what is considered a "sale of PHI" and defines it to mean a disclosure of PHI by a Covered Entity or Business Associate where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Defining the terms

An ***EXCHANGE*** of PHI is not limited to a transfer of ownership; if the Covered Entity or Business Associate is compensated for supplying the PHI to another party, a ***SALE*** has occurred.

REMUNERATION is not limited to financial payment; it includes nonfinancial benefits, including in-kind benefits.

A Covered Entity or Business Associate is prohibited from receiving direct or indirect remuneration in exchange for the disclosure of PHI, unless the individual's authorization is obtained, and such authorization must state that disclosure will result in remuneration to the Covered Entity or Business Associate.

Business Associates may recoup fees from third party record requestors for preparing and transmitting PHI on behalf of a Covered Entity, if the fees are reasonable, cost-based fees to cover the cost of preparing and transmitting the PHI or as otherwise expressly authorized by other law.

Exceptions to the rule are disclosures

- for treatment and payment purposes (including disclosures to a collection agency for purposes of payment collection activities);
- for certain public health purposes;
- for certain research purposes;
- as part of a sale, transfer, merger, or acquisition of a Covered Entity where the recipient is or will become a Covered Entity;
- to or by a Business Associate for activities that the Business Associate undertakes on behalf of a Covered Entity (or on behalf of a Business Associate in the case of a subcontractor), and where the only remuneration provided is by the Covered Entity to the Business Associate (or by the Business Associate to the subcontractor) for the performance of such activities;
- to an individual exercising HIPAA access or accounting rights; and
- as required by law.

Under these exceptions, there is no cap on the amount of payment the disclosing Covered Entity or Business Associate can receive.

Access to Protected Health Information

The Final Rule expands individuals' rights to receive copies of their PHI by requiring Covered Entities to provide access to PHI in the electronic form and format requested by the individual, if the PHI is maintained electronically in one or more designated record sets (e.g., enrollment, payment, claims, and medical billing records). If the Covered Entity cannot readily produce the form and format requested, it must offer other electronic formats that it can provide and is expected to provide a "machine readable" copy of the PHI including an electronic copy in MS Word, Excel, text, HTML, or PDF formats. If the individual does not agree to the alternative electronic formats offered, the Covered Entity must provide a hard copy as an option.

The Covered Entity must send the PHI to a designated third party if the individual submits a signed request identifying the designated recipient.

If the individual requests that a copy of his/her PHI be sent via unencrypted email, the Covered Entity is allowed to do so, as long as the Covered Entity has advised the individual of the risks and the individual still prefers the unencrypted email.

Electronic and hard copy PHI must be provided to an individual within 30 days of an individual's request, with one single 30-day extension if the Covered Entity provides notice to the individual of the delay and the expected date it will complete the request. Prior to the Final Rule, PHI had to be provided within 30 days (with a 60-day extension if PHI was maintained offsite) with one single 30-day extension. As such, the Final Rule shortened the time period from 90 days total to 60 days total.

Covered Entities are allowed to charge a reasonable and cost-based fee to cover the individual's access request.

> The Final Rule shortens the maximum time allowed for a Covered Entity to provide an electronic or hard copy of an individual's PHI following a request from the individual from ninety days total to sixty days.

Genetic and Decedent Information

Genetic Information

The Final Rule clarifies, in accordance with the Genetic Information and Non-Discrimination Act (GINA), that genetic information is health information and prohibits health plans (including limited-scope dental and vision plans) from using or disclosing genetic information for underwriting purposes. Underwriting purposes include

- enrollment, eligibility, and coverage determinations;
- computation of premium and contribution amounts;
- application of preexisting condition exclusions; and
- other activities related to placement of health insurance.

Individual authorization may **not** be used to allow a health plan to use or disclose genetic information for underwriting purposes.

Genetic information is defined to include manifestation of a disease or disorder in a family member of an individual in addition to genetic tests and requests for and receipt of genetic services. The **actual** manifestation of a disease or disorder in an individual is not considered genetic information and, as such, claims experience **can** be used to set premiums. On the other hand, genetic test results cannot be used to adjust premiums since tests results are not equivalent to claims experience.

Exceptions to the rule apply to allow

- issuers of long-term care policies to use genetic information for underwriting purposes; and
- health plans to use or disclose the minimum necessary genetic information about an individual to determine whether the provision of a particular benefit is medically necessary.

> If a health plan underwrites using genetic information, the plan will not only violate GINA and be subject to GINA penalties, but it will also violate HIPAA and be subject to much higher HIPAA penalties.

Decedent Information

The Final Rule limits the protection of deceased individuals' PHI to 50 years. Previously, there was no limit on the length of time such PHI was required to be protected.

The Final Rule also allows disclosure of a decedent's PHI to family, friends or other persons who were involved in the decedent's care or payment, unless such disclosure is contrary to the decedent's previously expressed preference. Previously, PHI could be disclosed to family, friends or other persons involved in the individual's care or payment before the individual died, but once the person died, PHI could only be disclosed to the decedent's personal representative (which was problematic when the decedent's estate was not open and the personal representative could not be located).

Notice of Privacy Practices

Content

Due to the changes the Final Rule made to the Privacy Rule, Covered Entities must update their Notice of Privacy Practices (NPP) and must include the following information:

- The sale of PHI and the use of PHI for paid marketing require authorization from the individual.
- Other uses and disclosures of PHI not described in the NPP will be made only with authorization.
- Covered Entities must notify affected individuals of breaches of their unsecured PHI.
- Individuals can restrict disclosures to their health plan for services they have paid for out-of-pocket and in full (only applies to providers' NPPs; other Covered Entities can use existing NPP language stating that the Covered Entity is not required to agree to a requested restriction).
- Individuals have the right to obtain an electronic copy of their PHI.
- Covered Entities that plan to contact individuals for fundraising purposes must inform individuals of this intent and of their rights to opt out of receiving any fundraising communications.
- Health plans that underwrite must state that the plan cannot use or disclose genetic information for underwriting purposes.
- Covered Entities that maintain psychotherapy notes must state that most uses and disclosures of such notes require authorization.

Distribution

Under the current NPP distribution requirements for health plans, the plan must provide the notice to an employee at the time that the employee first enrolls in the plan, and again – to all employees covered by the plan – within 60 days of a material revision to the notice. (The plan is not required to provide separate notices to dependents.)

The Final Rules modified the distribution requirements for health plans when there is a material revision to the NPP as follows:

If:	The Plan Must:
A health plan maintains a web site that provides information about the plan's customer services or benefits,	Prominently post the NPP on the web site and make the notice available electronically through the web site. In the event of a material change to the NPP, the health plan must prominently post the revised NPP on its website **and** provide the revised NPP or information about the material changes and how to obtain the revised NPP in its next annual mailing to covered employees (i.e. with open enrollment materials).
A health plan does not have a customer service website,	Provide the revised NPP, or information about the material changes and how to obtain the revised NPP, to covered employees within 60 days of the date of the revised NPP.
A health plan must also provide a paper copy of the notice upon an employee's request.	

Since health plans must comply with the Final Rule by September 23, 2013, the revised NPP must be effective the same date, and it must be distributed in accordance with the above rules for a material modification of an NPP as follows:

For Health Plans that:	The Plan Must:
Maintain a web site that provides information about the plan's customer services or benefits,	Prominently post the revised NPP on the website and make the notice available electronically through the web site by September 23, 2013; **and**
	Provide the revised NPP or information about the material changes and how to obtain the revised NPP in its next annual mailing to covered employees (i.e. with open enrollment materials).
Do not have a customer service website,	Provide the revised NPP, or information about the material changes and how to obtain the revised NPP, to covered employees by November 22, 2013 (which is within 60 days of the September 23, 2013 date of the revised NPP).

Health plans must still also provide a copy of the revised NPP to new employees at the time they enroll in the plan and, if the plan posts the NPP to its website, it must also provide a paper copy upon an employee's request. In addition, no less frequently than once every three years, the plan must notify employees then covered by the plan of the availability of the notice and how to obtain the notice.

Breach Notification Rule

Definition of Breach and Risk Assessment Approach

The Final Rule modified the definition of "breach" and the risk assessment process set forth in the Interim Final Breach Notification Rule issued by HHS on August 24, 2009. The Interim Rule defined a breach as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI", unless an exception applied. The Interim Rule used the harm standard in applying this definition and further defined the phrase "compromises the security or privacy of the PHI" to mean "poses a significant risk of financial, reputational, or other harm to the individual". In order to determine if an impermissible use or disclosure of PHI constituted a breach, a Covered Entity or Business Associate, as applicable, was required to perform a risk assessment to determine if there was a significant risk of harm to the individual.

Under the Final Rule's new definition of "breach", an impermissible acquisition, access, 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." HHS has indicated that the prior "harm to an individual" standard was too subjective, presenting inconsistent interpretations and results across Covered Entities and Business Associates.

_Re_-Defining the terms

A ***BREACH*** has been redefined to refer to an impermissible acquisition, access, use or disclosure of PHI 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."

This new definition is intended to remove the subjectivity inherent in the previous "harm to an individual" standard.

The Final Rule provides for a more objective standard and requires the following factors to be used in assessing the probability of whether PHI was compromised:

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (e.g. determine if highly-sensitive information was disclosed, such as Social Security numbers, mental health records or infectious disease test results; or if the PHI could be used in a manner "adverse" to the individual or for the recipient's own interests)
- the identity of the unauthorized person who used the PHI or to whom the disclosure was made (e.g. determine if the person or entity has a corresponding obligation to protect the information, such as another physician; or if the recipient is capable of re-identifying the data)

- whether the PHI was actually acquired or viewed (e.g. if PHI on recovered laptop was not viewed, accessed, or transferred, then there is no breach)
- the extent to which the risk to the PHI has been mitigated (e.g. determine if the PHI was immediately destroyed; or if the recipient signed a confidentiality agreement assuring that the PHI will not be used or disclosed)

HHS also indicated that, depending on the circumstances, it might be appropriate to consider other factors in the risk assessment.

Exceptions to Definition of Breach

Under the Interim as well as the Final Rule, if an exception to the definition of "breach" applies, then a breach has not occurred, and neither a breach analysis nor notification is required. The Final Rule maintained all the following exceptions to the definition of breach set forth in the Interim Rule:

- The data was encrypted and access to the encryption key was not compromised.
- The data was sent to another Covered Entity that properly disposed of the data.
- Although the data was disclosed to an unauthorized person, the unauthorized person would not reasonably be able to retain it.
- The data disclosed represented unintentional access, acquisition, or use by a workforce member.

The Final Rule did **not** maintain the exception for limited data sets under the Interim Rule. Under the Interim Rule, if data was contained in a Limited Data Set with dates of birth and ZIP codes removed and with no risk of re-identification, a breach did not occur. Under the Final Rule, disclosure of PHI contained in a Limited Data Set with dates of birth and ZIP codes removed is presumed to be a breach and a risk assessment is required to determine if an actual breach occurred.

Notifications

The Final Rule did not change the content requirements or the methods of notification for breaches. However, clarification for notices to the media and to HHS were included as follows:

Notification to the Media

Covered Entities are not required to incur any costs to run print or media notices, nor are media outlets obligated to print or run such notices. The posting of a press release on a Covered Entity's website does not fulfill the requirements for media notification. Rather, the required notification must be provided directly to the media outlet where the affected individuals reside.

Notification to the Secretary of HHS

If a data breach affects **fewer than 500 individuals**, Covered Entities must notify the Secretary of HHS no later than 60 days after the end of the calendar year in which the breach was **discovered**, not in the year the breach occurred.

If a breach affects **500 or more individuals**, the requirement for a Covered Entity to "immediately" report to HHS means that the notification should be made contemporaneously with the Covered Entity's notice to individuals.

The Final Rule also includes updated guidance on the discovery and reporting of breaches by a Business Associate and Covered Entity as follows:

- The Business Associate must notify the Covered Entity within 60 days of discovery of a breach; then the Covered Entity has 60 days to notify the individual.
- If the Business Associate is an agent of the Covered Entity, the Covered Entity has 60 days total from the date the Business Associate discovers the breach.
- The Covered Entity is ultimately responsible to perform a risk assessment, determine if a breach has occurred and provide the required notifications.

Enforcement

The Final Rule strengthens HIPAA's enforcement provisions, which are expected to result in more aggressive HIPAA enforcement. The following provisions are contained in the Final Rule:

- HHS is no longer required to attempt to resolve a HIPAA violation through informal means, such as through voluntary compliance by the entity that committed an alleged violation.
- HHS is now obligated to conduct a formal investigation of a HIPAA complaint where a preliminary review indicates a possible, not just probable, violation due to "willful neglect", and must also conduct a compliance review to investigate a possible HIPAA violation brought to its attention through less formal means.
- HHS has the discretion to resolve HIPAA violations by informal means; however, HHS may directly move to a Civil Monetary Penalty (CMP) without informal resolution when HHS determines that noncompliance is due to "willful neglect".
- Business Associates (including their subcontractors) are now subject to CMPs and other enforcement actions for noncompliance with applicable provisions of HIPAA. Business Associates (like Covered Entities) may also be liable for violations of their agents.
- The amount of CMPs is harsher under the Final Rule and increase under a tiered structure based on the degree of culpability of the violation, ranging from "Did Not Know" to "Willful Neglect – Not Corrected". The penalties range from $100 to $50,000 per occurrence, with the maximum amount reaching $1.5 million for violations of an identical provision in the same calendar year. The Secretary of HHS retains the discretion on the level of penalty to assess and will consider the following factors in its determination:
    - the nature and extent of the harm resulting from the violation, including the number of individuals affected and the duration of the violation
    - the nature and extent of any individual's resulting physical, financial or reputational harm, including any hindrance to the individual's ability to obtain health care
    - the history of prior compliance with HIPAA's administrative simplification provisions by the Covered Entity or Business Associate that committed the violation
    - the financial condition of the Covered Entity or Business Associate that committed the violation, including difficulties that could have affected compliance or that could cause a monetary penalty to jeopardize the future provision of health care
    - other matters as justice may require

The following chart outlines the applicable CMPs by degree of culpability.

Violation Category Penalty	**CMP Range** ***(per Violation)***	**Maximum Penalty for all Violations of Identical Provisions in a Calendar Year**
Entity **did not know and would not have known** (by exercising reasonable diligence) that it violated the applicable provision.	$100 – $50,000	$25,000 (if $100 penalty) up to $1,500,000 (if $50,000 penalty)
Violation is **due to reasonable cause and not willful neglect.**	$1,000 – $50,000	$100,000 (if $1,000 penalty) up to $1,500,000 (if $50,000 penalty)
Violation is **due to willful neglect and was corrected during 30-day period** beginning on the first date the entity knew, or would have known (by exercising reasonable diligence) that the violation occurred.	$10,000 – $50,000	$250,000 (if $10,000 penalty) up to $1,500,000 (if $50,000 penalty)
Violation is **due to willful neglect and was not corrected during 30-day period** beginning on the first date the entity knew, or would have known (by exercising reasonable diligence) that the violation occurred.	At least $50,000	$1,500,000

Defining the terms

REASONABLE CAUSE is an act or omission in which a Covered Entity or Business Associate knew, or by exercising reasonable diligence would have known, that the act or omission violated HIPAA but in which the Covered Entity or Business Associate did not act with willful neglect.

WILLFUL NEGLECT is a "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA.

Other possible enforcement provisions include:

- criminal penalties of up to 10 years' imprisonment; and
- state Attorneys General can bring a civil action on behalf of a State resident of up to $100 per violation, with cap of $25,000 for identical violations in a calendar year.

Implementation

Health Plans' actions

As a Business Associate of your group health plan ("Plan") (the Covered Entity), **Health Plans, Inc.** maintains compliance with the HIPAA Privacy, Security and Breach Notification Rules in order to protect the privacy and provide for the security of members' protected health information. **Health Plans** has an extensive set of HIPAA Privacy & Security Policies and Procedures in place as well as a Written Information Security Plan (WISP) which are reviewed and modified, as applicable, on an annual basis by our Privacy Officer and Security Officer. New employees are trained on the policies and procedures and all employees undergo annual HIPAA training. **Health Plans** understands that we are directly liable for HIPAA violations in accordance with the Final Omnibus Rule ("Final Rule"), and we will continue to comply with all applicable regulations. Specifically, with regard to the Final Rule we will take the following actions:

- **Business Associate Agreements**

  Health Plans currently has a Business Associate Agreement in place with your Plan (Addendum I to the Administrative Services Agreement) which contains all required provisions in accordance with the HIPAA Privacy and Security Rules as well as the HITECH Act and the Interim Final Breach Notification Rules. We have reviewed the provisions of our Business Associate Agreement to determine if any revisions are necessary due to the requirements of the Final Rule and have determined that no revisions are necessary since our current version was drafted in anticipation of the requirements of the Final Rule and it contains all required provisions. As such, we will not be issuing an amendment to the Agreement.

  Health Plans also currently has Privacy & Data Security Agreements and/or Confidentiality & Nondisclosure Agreements in place with all of our subcontractors which contain all required provisions of the HIPAA Privacy and Security Rules, HITECH Act and the Interim Final Breach Notification Rules. As with our Business Associate Agreements, we drafted our subcontractor Agreements in anticipation of the requirements of the Final Rule and they also contain all required provisions. As such, our subcontractor Agreements do not need to be amended.

- **Privacy and Security Policies and Procedures**

  We will update our Privacy and Security Policies and Procedures to include the applicable requirements of the Final Rule, including

  - provisions for "marketing" and "sale" of PHI;
  - procedures for granting individuals access to their electronic records;
  - procedures to ensure that genetic information is not used for underwriting purposes; and
  - procedures for disclosing and retaining decedent information.

- **Notice of Privacy Practices**

  We will update our Notice of Privacy Practices ("NPP") on your Plan's behalf in accordance with the Final Rule and we will post it to our website in a location where it is prominently displayed to your Plan members. Members will also be able to print a paper copy from the website.

  We are in the process of revising the NPP and will notify you as soon as it is ready. We will also email a copy to you so that you can provide it to your employees with your next annual open enrollment materials and upon an employee's request. Health Plans will continue to provide the NPP to new enrollees in your Plan, and it will be included in the new member kits we send out. If your Plan does not use the Health Plans template NPP, please contact your Account Manager to discuss the posting and distribution procedure you would like.

- **Breach Notification Policy and Procedure**

  We will update our Breach Notification Policy and Procedure to include the applicable requirements of the Final Rule, including

  - modified definition of a "breach";
  - exceptions to the definition of "breach";
  - revised risk assessment process;
  - revised media and HHS notification; and
  - revised discovery and reporting time periods.

- **Workforce Training**

  We will provide training to our employees on the applicable requirements of the Final Rule, including our updated Policies and Procedures.

Employer's actions

Since your Plan is a Covered Entity, you will need to take steps to ensure compliance with the Final Rule, including:

- Review current Business Associate Agreements in place with the Plan's Business Associates to ensure all required provisions are included in accordance with the Final Rule. If an amendment to specific Agreements is necessary, ensure the amendment is processed per the transition rule (see the *Business Associate Agreements – Content* section above on page 5 for the transition rule requirements).
- Confirm Business Associate Agreements are in place with all of the Plan's Business Associates. If not, ensure an Agreement is in place **no later than September 23, 2013**.
- Update the Plan's Privacy and Security Policies and Procedures to include the applicable requirements of the Final Rule, including
    - provisions for "marketing" and "sale" of PHI;
    - procedures for granting individuals access to their electronic records;
    - procedures to ensure that genetic information is not used for underwriting purposes; and
    - procedures for disclosing and retaining decedent information.
- Update the Plan's Breach Notification Policy and Procedure to include the applicable requirements of the Final Rule, including
    - modified definition of a "breach";
    - exceptions to the definition of "breach";
    - revised risk assessment process;
    - revised media and HHS notification; and
    - revised discovery and reporting time periods.
- Train your workforce on the applicable requirements of the Final Rule, including the Plan's updated Policies and Procedures.