February 28, 2013

At issue

AN EMPLOYEE BENEFITS REGULATORY AFFAIRS BULLETIN • *Karen R. Mcleese, Esq.*

In This Special Edition:

HIGHLIGHTS OF FINAL HIPAA REGULATIONS:

- MODIFICATION AND RE-DISTRIBUTION OF NOTICE OF PRIVACY PRACTICES
- INDIVIDUAL RIGHTS
- WRITTEN AUTHORIZATIONS
- INTERPLAY OF HIPAA AND GINA
- BREACH NOTIFICATION
- BUSINESS ASSOCIATES
- ENFORCEMENT
- NEXT STEPS FOR COVERED ENTITIES

In 2009, the *Health Information Technology for Economic and Clinical Health* (HITECH) Act became law. Nearly four years later, ***comprehensive regulations*** have been issued interpreting this law. In addition, these regulations further clarify breach notification rules that were issued on August 24, 2009 and address privacy issues deriving from the *Genetic Information Nondiscrimination Act of 2008* ("GINA"). Following is a summary of some pertinent parts of the regulations as they relate to a health plan as a covered entity.

As background, administrative simplification standards were enacted as part of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) and include three components: health care privacy rules, electronic data interchange (EDI) rules, and security of health data rules. The HITECH law added rules relating to breach notification.

- The HIPAA privacy rules govern how individually identifiable medical information must be protected. These rules became applicable to large plans on April 14, 2003; and, April 14, 2004 for small plans with fewer than $5 million in premium.
- The HIPAA security rules require that administrative, physical, and technical safeguards be established to ensure the security of protected health information held in electronic form (e-PHI). These rules became effective on April 21, 2005 for large plans; April 21, 2006 for small plans.
- The HITECH Act requires covered entities to notify affected individuals in the event of a breach of their unsecured health information. These regulations became effective on September 23, 2009; however, HHS honored a "non-enforcement policy" through February 24, 2010. For many purposes, HITECH brings Business Associates under the direct jurisdiction of the law, as more fully described below.

Continued from Page 1

The HIPAA privacy, security and breach notification rules require covered entities, defined as health plans, health plan clearinghouses and health care providers, to ensure the protection of protected health information (PHI). PHI includes any individually identifiable medical information maintained in any form, including electronic and oral communications, that:

- Is created or received by a covered entity;
- Relates to an individual's physical or mental condition, the provision of health care services to such individual, or the payment for such health care services; or,
- Identifies the individual or creates a reasonable basis to believe that such information could be used to identify the individual.

NOTICE OF PRIVACY PRACTICES: MODIFICATION AND RE-DISTRIBUTION

A covered entity is required to maintain a notice of its privacy practices (NPP). A Business Associate is not required to maintain NPP, unless required by the terms of a Business Associate agreement. For an insured plan, it is generally the insurer that is the covered entity, and thus responsible for maintenance and distribution of NPP.

The NPP must include certain elements to inform individuals of how their PHI may be used or disclosed. The final regulations require additional information be contained in the NPP:

1. A description of the types of uses and disclosures that require written authorization for releasing PHI when it involves:
   - Psychotherapy notes; and
   - For marketing purposes or the sale of PHI where the covered entity receives financial remuneration from a third party (this information must also be included in the authorization provided to the individual).
2. A statement that other uses and disclosures not described in the NPP will be made only with the individual's written authorization.
3. A statement explaining how an individual may revoke an authorization.
4. If the covered entity is a health plan and intends to use or disclose PHI for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing any genetic information about the individual for such purpose.
5. A statement that the covered entity is required by law to maintain the privacy of PHI, to provide individuals with notice of its legal duties and privacy practices with respect to PHI, and to notify affected individuals following a breach of unsecured PHI.

Redistribution of the NPP

Currently, there are certain timeframes and instances in which a covered entity must provide its NPP to participants, such as at the point the individual becomes covered under the plan, as well as a triennial notification requirement. It is also required to be provided within 60 days of any material changes to the content of the NPP.

Due to the additional information required to be included in the NPP, covered entities must re-distribute their revised NPP in the following timeframes and methods:

- Covered entities/health plans may either prominently post the material changes of their NPP, or post and provide the revised NPP on its website. This must be accomplished by the effective date of the material change to the NPP. In addition, information about the material change and how to obtain the revised NPP must be included in its next annual enrollment materials distributed to participants.

- Covered entities/health plans that do not utilize a website for posting their NPP must provide the revised NPP, or information about the material change and how to obtain the revised NPP to participants, within 60 days of the material revision to the NPP.
- For new enrollees of a health plan, the NPP must be provided at the time of enrollment.

The NPP can be delivered electronically to individuals, as long as the individual agrees to electronic delivery and is notified of the right to obtain a paper copy of the NPP upon request.

INDIVIDUAL RIGHTS

The final rules strengthen rights of individuals with regard to their PHI in the following ways:

- *Access to PHI.* Under HIPAA, individuals have a right to receive an electronic copy of their PHI. The final rules require that if the individual requests an electronic copy of his/her PHI that is maintained in one or more designated record sets, the covered entity must provide access to the electronic version if the individual requests it. If the electronic version is not readily producible, the covered entity may charge a fee for costs associated with labor and supplies for creating an electronic copy, including postage or courier costs. However, covered entities cannot include fees associated with maintaining systems, retrieval costs, or infrastructure costs associated with providing electronic copies.

- *Right to Restrict Certain Disclosures to a Health Plan*. The final rule requires health care providers to honor an individual's request to restrict disclosure of his/her PHI to a health plan in the event the individual pays the full out-of-pocket amount (i.e., outside the plan) for a particular health care service. Under the prior rules, a health care provider was given the option to comply with the request. The health care provider is not required to separate or segregate records in order to ensure the individual's restriction request is honored; rather it is up to the provider's discretion as to how to flag the restricted information.

- *Authorization for Uses and Disclosures of PHI for Marketing and Sale Activities*. As mentioned above, individuals must authorize use and disclosure of their PHI when used in marketing and sale activities by the covered entity receiving remuneration. The right of an individual to opt out of fundraising communications must be clearly communicated, and should be treated as a revocation of authorization.

WRITTEN AUTHORIZATION REQUIRED

If PHI is to be used for other than payment, treatment or health care operation, generally, an individual must authorize any disclosure. The final rules strengthen the limitations on the use and disclosure of PHI for marketing and fundraising purposes, and prohibit the sale of PHI without individual authorization. An individual's written authorization is required for releasing his/her PHI when it involves:

- Psychotherapy notes; or
- Marketing communications or the sale of PHI where the covered entity receives financial remuneration from a third party.

The authorization must include an explanation of how an individual may revoke an authorization.

In addition, the rules modify instances in which it is permissible to disclose PHI without an individual's authorization:

- To facilitate research;
- To permit disclosure of child immunization proof to schools in the event a state requires immunization records to be disclosed to schools;

- To permit disclosure amongst covered entities participating in the same organized health care arrangement; and
- To enable access to decedent information by family members or others as long, as it is consistent with the prior express wishes of the deceased.

GENETIC INFORMATION

Consistent with the *Genetic Information Nondiscrimination Act of 2008*, the final rules make clear that:

- Genetic information is PHI; and
- Health plans (excluding long term care policies) cannot use or disclose genetic information for such underwriting purposes as:
  - Determining eligibility or benefits under the plan;
  - Premium or contribution differentials;
  - Application of preexisting condition exclusions; or
  - Other actions relating to renewal or replacement of the plan or policy.

BREACH NOTIFICATION

In the event of a breach of unsecured PHI, affected individuals must be notified of the breach, without unreasonable delay, and in no event more than 60 days following discovery of the breach. According to current law, all PHI is unsecured unless it is encrypted or destroyed.

Historically, a breach notification was required when the breach posed a significant risk of financial, reputational, or other harm to the individual. These final regulations change the 'risk of harm' standard to a 'low probability' standard. Following a breach, a risk assessment of potential vulnerabilities to the confidentiality, integrity, and availability of e-PHI must be accomplished. A breach notification obligation would be triggered unless it is determined that there is a low probability that harm to affected individuals would occur.

Factors used in this 'low probability' determination include:

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 burden of proof is on the covered entity and/or business associate to determine potential harm of misappropriated e-PHI.

Types of Breach Notifications

There are potentially three breach notices that may be required: an individual notice, a notice to the media, and a notice to the HHS Secretary. In addition, a business associate has an obligation to report a breach to the covered entity.

INDIVIDUAL NOTICE

Affected individuals must be notified, in writing, in the event of a breach of their unsecured PHI. Covered entities are required to notify affected individuals of the breach without unreasonable delay, but in no event later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay.

NOTICE TO MEDIA

When a breach involves more than 500 residents of a State or jurisdiction, the rules prescribe the timing of breach notification that must be provided to prominent media outlets serving the State or jurisdiction.

NOTICE TO HHS SECRETARY

In addition to notifying affected individuals and media as described above, a covered entity must maintain a breach notification log.

- If the breach affects 500 or more individuals, the Secretary of Health and Human Services must be notified immediately. Further, the ***HHS Office of Civil Rights website*** (OCR) provides how this notice must be accomplished.
- If the breach involves fewer than 500 individuals, the covered entity's log must be submitted to HHS Secretary via OCR's website (as above) within 60 days following the close of the calendar year in which the breach is discovered, rather than when it occurs. This modification does not alter a covered entity's obligation to promptly report the breach to affected individuals without unreasonable delay, but in no event later than 60 calendar days after discovery of the breach.

BREACH NOTIFICATION BY BUSINESS ASSOCIATE

Following the discovery of a breach of unsecured PHI, a business associate must notify the covered entity of such breach. A breach is deemed discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate.

BUSINESS ASSOCIATES

The HITECH law makes business associates subject to a significant portion of the collective privacy and security rules. These regulations re-define a business associate as:

- A person who, on behalf of a covered entity, creates, receives, maintains, or transmits PHI for a function or activity, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing.
- A person who provides any legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a covered entity other than in the capacity of a member of such covered entity's workforce. This could include services involving disclosure of PHI within an organized health care arrangement. For these purposes, *workforce* includes employees, volunteers, trainees, and other persons who are employed by and under direct control of the business associate.

The final regulations add three distinct categories of business associates:

1. A Health Information Organization, E-prescribing Gateway, or other entity providing data transmission services involving routine access to PHI for a covered entity.
2. A person that offers a personal health record to individuals on behalf of a covered entity.
3. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. Further, the regulations make it clear that any subcontractor of the business associate must agree, in writing, to the terms and conditions of the business associate agreement.

A covered entity may be a business associate of another covered entity. An individual or entity that is assisting the business associate with its own business practices and not the activities of the covered entity, would not, on the other hand, be considered a business associate.

A business associate also *does not* include:

- A health care provider when receiving PHI by a covered entity relating to treatment of an individual.

- A plan sponsor of a group health plan when receiving PHI for purposes of carrying out administrative functions of the plan.
- Government agencies sharing information to determine eligibility in public health benefit programs.
- A covered entity participating in an organized health care arrangement that performs a function, activity or service on behalf of the arrangement.

Obligations of Business Associates

Business associates are obligated to:

1. Not use or disclose PHI other than as permitted or required by the business associate agreement, or as required by law.
2. Comply with the security rules relating to safeguarding e-PHI.
3. Report any use or disclosure of PHI to covered entity when it becomes aware, including breaches of unsecured PHI and any security incidents.
4. Ensure that any subcontractors who create, receive, maintain, or transmit PHI on behalf of the business associate comply with the same restrictions, conditions, and requirements that apply to the business associate.
5. Make PHI available in a designated record set to the covered entity or individual as necessary to satisfy covered entity's obligations, as well as make any amendments to PHI in a designated record set, as directed or agreed to by the covered entity.
6. Maintain and make available the information required to provide an accounting of disclosures to the either the covered entity or individual, as necessary to satisfy covered entity's obligations.
7. Make its internal practices, books, and records available to OCR for purposes of determining compliance with the HIPAA Rules.

Business Associate Agreements

Covered entities are required to enter into business associate agreements with business associates, including third party administrators (TPAs), premium administrators, accountants, attorneys, consultants, utilization review entities, and any other entity that engages in a function governed by HIPAA, or with access or use of PHI. The intent of this requirement is to ensure that business associates would likewise provide safeguards to PHI. The final regulations require business associates, in turn, to enter into business associate agreement(s) with any downstream subcontractors.

In conjunction with the final HIPAA final regulations, the OCR has posted a ***sample business associate agreement*** on its website. It is important for covered entities to carefully review this sample language to ensure its appropriateness in respect to the business associate relationship between a covered entity and its business associate, or between a business associate and its subcontractor.

REQUIRED COMPONENTS OF BUSINESS ASSOCIATE AGREEMENTS. Business associate agreements must set forth provisions relating to:

1. Permitted and required use and disclosures of PHI by the business associate.
2. Minimum necessary standards that limit the use or further disclosure of PHI other than as permitted or required by the agreement, or as required by law.
3. Implementation of appropriate safeguards to prevent unauthorized use or disclosure of the information, including e-PHI.
4. Obligation to report any use or disclosure of the information not provided by the agreement to the covered entity, including incidents that constitute breaches of unsecured PHI.

5. Disclosure of PHI in accordance with the agreement in order to satisfy a covered entity's obligation regarding an individual's request for copies of his/her PHI, as well as make PHI available for amendments and accountings.
6. Obligation to make the business associate's internal practices, books, and records relating to the use and disclosure of PHI available to HHS for purposes of determining the covered entity's compliance.
7. Obligation of the business associate to ensure that any subcontractors it may engage on its behalf with access to PHI agrees to the same restrictions and conditions that apply to the business associate.
8. At termination of the agreement, require the business associate to return or destroy all PHI received or created by the business associate on behalf of the covered entity.
9. Authorizing termination of the agreement by the covered entity if the business associate violates a material term of the agreement.

New business associate agreements entered into on or after January 25, 2013 must include the above provisions by September 23, 2013.

A business associate agreement in force on January 25, 2013 will have until September 22, 2014 to make the agreement compliant, as long as no significant modifications are made to the agreement prior to that date. This delay notwithstanding, compliance with the regulations is required as of September 23, 2013.

Enforcement of HIPAA Privacy, Security and Breach Notification Violations

Enforcement of the HIPAA privacy, security and breach notification rules is delegated to the HHS Office for Civil Rights, in collaboration with the U. S. Department of Justice. In addition, the HITECH law authorized enforcement of privacy violations by State attorneys general. These agencies may begin investigations of violations by reviewing submitted complaints, by performing a compliance review or audit, and by reviewing breach reports.

In the event of a violation, not only are health plans, providers and clearinghouses subject to civil and criminal penalties, but appropriate sanctions may also be taken against workforce members and subcontractors who fail to comply with the policies and procedures of the covered entity or business associate.

Both OCR and State Attorneys General may impose separate civil penalties of up to $100 per violation, or up to $25,000 for identical violations during a calendar year. With regard to breach violations, the final regulations adopt the four proposed tiers of civil penalties that could be imposed upon covered entities, depending on the nature of the violation. Criminal penalties, including fines and imprisonment, may also be imposed by the U. S. Department of Justice.

Compliance Date

Covered entities and business associates must comply with the applicable requirements of this final rule by September 23, 2013.

NEXT STEPS

- Note, an employer, itself, is not a covered entity. The health plan(s) is the covered entity.

- For Covered Entities:
  1. Identify health plan(s)
     - If a plan is insured and the employer receives no PHI, make certain the insurer is compliant with HIPAA, including distribution of the NPP.
     - If a plan is self-funded, identify business associates and subcontractors, such as a third party administrator, a utilization review organization, or an entity providing legal or accounting functions on behalf of the plan.
  2. Review and update Business Associate agreements.
  3. Review and update HIPAA policies and practices, including security rules for any e-PHI.
  4. If PHI is maintained, make certain it is kept confidential.
  5. If e-PHI is maintained, make certain it complies with security rules.

About the Author: Karen R. McLeese is Vice President of Employee Benefit Regulatory Affairs for CBIZ Benefits & Insurance Services, Inc., a division of CBIZ, Inc. She serves as in-house counsel, with particular emphasis on monitoring and interpreting state and federal employee benefits law. Ms. McLeese is based in the CBIZ Leawood, Kansas office.