BEACON Specialized Living

Compliance Steps for the Final HIPAA Rule

On Jan. 25, 2013, the Department of Health and Human Services (HHS) issued a final rule under HIPAA's administrative simplification provisions. The final rule updates HIPAA's privacy, security, enforcement and breach notification requirements, and includes changes required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

This Legislative Brief provides an overview of key changes made by the final HIPAA rule and outlines compliance steps for health plans.

OVERVIEW

The final HIPAA rule creates new requirements for health plans and their business associates. To highlight important changes, the final rule:

- Makes business associates directly liable for complying with certain portions of the HIPAA Privacy and Security Rules;
- Revises the HITECH Act's breach notification requirements for unsecured protected health information (PHI) to replace the "significant harm" threshold with a more objective standard; and
- Modifies certain aspects of the HIPAA privacy standards and requires covered entities to revise their privacy notices.

The deadline for complying with the changes made by the final HIPAA rule is Sept. 23, 2013. However, there is an extended compliance deadline for updating existing business associate agreements.

Covered entities will need to take steps to comply with the new requirements under the final rule.

To comply with the final rule, health plans will need to review and make necessary updates to:

→

- ✓ **Business associate agreements**
- ✓ **Some HIPAA policies and procedures (not all)**
- ✓ **Workforce training programs**
- ✓ **Privacy notices**

In light of HHS' increased enforcement of the HIPAA Privacy and Security Rules since the HITECH Act was enacted, covered entities should take their HIPAA compliance obligations seriously and periodically review whether they are adequately protecting the privacy and security of Protected Health Information (PHI).

Note: ALL electronic devices (cell phones, tablets, laptops, etc.) MUST be password-protected.

PLAN SPONSOR OBLIGATIONS

The extent of a plan sponsor's privacy and security obligations under the HIPAA rules largely depends on how the health plan is funded (insured or self-funded) and whether the sponsor has access to PHI for plan administration. Sponsors of self-funded plans must generally comply with the entire scope of privacy and security provisions for health plans. Sponsors of insured plans that do not have access to PHI (other than summary health information and enrollment and disenrollment information) have minimal obligations under the HIPAA rules; the health insurance issuer has the primary compliance obligation in this situation.

BEACON Specialized Living

Compliance Steps for the Final HIPAA Rule

Type of Plan	Extent of Plan Sponsor's HIPAA Privacy/Security Obligations
Self-funded	Full scope of HIPAA's privacy and security requirements for group health plans apply to the plan
Fully insured	If the plan does not create or receive PHI (other than summary health information and enrollment and disenrollment information), health insurer has the primary compliance obligation

FINAL HIPAA RULE
Changes for Business Associates

Expanded Definition

The final HIPAA rule expands the definition of "business associate" to generally include all entities that create, receive, maintain or transmit PHI on behalf of a covered entity, including subcontractors. According to HHS, including subcontractors in the definition of "business associate" will ensure that the HIPAA privacy and security protections for PHI do not lapse merely because a function is performed by a subcontractor rather than an entity with a direct relationship with a covered entity.

Under the final rule, the business associate that contracts with the subcontractor, and not the covered entity, is required to enter into a business associate agreement with the subcontractor. Under the final rule, a covered entity must obtain satisfactory assurances (through a business associate agreement) from its business associates that they will appropriately safeguard PHI. Business associates must do the same with regard to their subcontractors and so on, no matter how far "downstream" the information flows.

Also, the final rule clarifies that entities that store PHI, in hardcopy or electronic format, are business associates even if they do not access, use or disclose that information.

Direct Liability

The HITECH Act amended HIPAA to make many privacy and security provisions directly applicable to business associates. The final HIPAA rule clarifies the privacy and security provisions that directly apply to business associates, and notes that business associates are directly liable for failing to comply with these requirements. Business associates are directly responsible for complying with:

- The HIPAA Security Rules' administrative, physical and technical requirements for safeguarding electronic PHI and implementing policies and procedures for protecting electronic PHI;
- The Privacy Rules' restrictions on the use and disclosure of PHI; and
- The terms of a business associate agreement related to the use and disclosure of PHI.

In addition, business associates are directly responsible for:

- Reporting breaches of unsecured PHI to a covered entity in compliance with HIPAA's breach notification requirements;
- Providing PHI to HHS upon demand so that HHS may investigate and determine the business associate's compliance with HIPAA;
- Making reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request;

- Disclosing PHI to the covered entity, individual or individual's designee as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of PHI; and
- Entering into business associate agreements with subcontractors that create or receive PHI on their behalf.

Compliance Steps

Covered entities, including health plans, will need to **review their business associate agreements** to determine if they must be updated for the final HIPAA rule. For example, among other changes, the final HIPAA rule requires business associate agreements to state that a business associate will ensure that any subcontractors that create or receive PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information. Business associates will also be required to review their contracts with subcontractors that create or receive PHI to determine if updates are necessary.

HHS has provided sample business associate agreement language for covered entities and business associates to use as a starting point in drafting their own agreements.

The final HIPAA rule includes an important **transition rule** for business associate agreements that were in entered into prior to Jan. 25, 2013 and complied with the HIPAA requirements in effect on that date. The transition period allows existing agreements that are not renewed or modified between March 26, 2013 and Sept. 23, 2013 to remain compliant until **Sept. 23, 2014** or, if earlier, the date the agreement is renewed or modified after Sept. 23, 2013.

The transition rule extends the time for the paperwork only—it does not extend the time allowed for the covered entity and business associate to comply with the changes made by the final HIPAA rule.

Breach Notification

Objective Standard for Breach Determination

The HITECH Act requires covered entities to notify affected individuals following the discovery of a breach of unsecured PHI. Notification must also be provided to HHS and, in some cases, to the media.

The HITECH Act defines a "breach" as the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the information. There are three exceptions to this definition:

- Disclosures where the recipient of the information would not reasonably have been able to retain the information;
- Certain unintentional acquisition, access or use of information by employees or others acting under the authority of a covered entity or business associate; and
- Certain inadvertent disclosures among people similarly authorized to access PHI at a business associate or covered entity.

An interim final rule released in 2009 provided that a breach will compromise the security or privacy of PHI if it poses a significant risk of financial, reputational or other harm to the individual. Effective Sept. 23, 2013, the final rule replaces the "significant harm" threshold under the interim final rule with a more objective standard.

Under the final rule, an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates through a risk assessment that there is a **low probability** that the PHI has been compromised (or one of the three exceptions to the definition of breach applies). The risk

assessment must, at a minimum, take into account the following factors:

- The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

If an evaluation of the factors fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required.

Compliance Steps

To prepare for compliance with the final HIPAA rule, covered entities and business associates should examine their breach notification policies to ensure that they consider all of the required factors when evaluating the risk of an impermissible use or disclosure. Additional factors may also need to be considered based on the circumstances of the impermissible use or disclosure.

In addition, workforce training programs should be updated to include the new risk assessment and explain the factors to be considered in the assessment.

HIPAA Privacy Standards and Privacy Notice

New Privacy Standards

The final HIPAA rule makes certain modifications to HIPAA's privacy standards for PHI, including requiring covered entities to update their notice of privacy practices. For example, under the final rule:

- Covered entities must provide an individual with 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;
- Covered entities must agree to an individual's request to restrict PHI if the information pertains to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid in full;
- Covered entities must protect the PHI of a deceased individual for 50 years after the individual's death;
- Covered entities must comply with additional restrictions on the marketing and sale of PHI; and
- Health plans are prohibited from using or disclosing PHI that is genetic information for underwriting purposes (long-term care plans are exempt), as required by the Genetic Information Nondiscrimination Act of 2008 (GINA).

Under the final HIPAA rule, "underwriting purposes" means rules for eligibility (including enrollment and continued eligibility) for benefits under the plan, the computation of premium or contribution amounts under the plan, the application of any pre-existing condition exclusion under the plan or other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

Privacy Notice

In addition, the final HIPAA rule requires covered entities to revise and redistribute their HIPAA privacy notices. In general, a covered entity's privacy notice must describe the uses and disclosures of PHI that a covered entity is permitted to make, the covered entity's legal duties and privacy practices with respect to PHI and an individual's rights concerning PHI. The final HIPAA rule requires the privacy notice to also include:

- A description of certain types of uses and disclosures that require an individual's authorization (such as uses and disclosures of PHI for marketing purposes) and a statement that other uses and disclosures not described in the privacy notice will be made only with an individual's authorization;
- A statement that the covered entity is required to notify affected individuals of breaches of unsecured PHI; and
- For health plans that engage in underwriting activities, a statement that the covered entity is prohibited from using or disclosing PHI that is genetic information for underwriting purposes.

A covered entity that updated its privacy notice for the HITECH Act and distributed it does not need to revise and distribute the notice again, provided the notice already includes the information required by the final rule.

Compliance Steps

In light of the final HIPAA rule, covered entities should review their HIPAA privacy policies and procedures and make any necessary updates to make sure they are consistent with the new privacy standards. Employees working with PHI should also be trained on the new standards. In addition, covered entities must review their privacy notices, make the required updates and distribute the updated notices.

The final rule includes important provisions for distributing privacy notices.

- A health plan that posts its privacy notice on its website must post the material changes or its revised notice on the website by Sept. 23, 2013, and provide the revised notice (or information about the material change and how to obtain the revised notice) in its next annual mailing to plan participants, such as during the plan's open enrollment period.
- A health plan that does not have a website must provide the revised notice (or information about the material change and how to obtain the revised notice) within 60 days of the material revision to the notice.

Also, it is important to remember that issuers of fully insured health plans have the primary responsibility for the privacy notice and sponsors of these plans have limited responsibilities with respect to the notice. If the sponsor of a fully insured plan has access to PHI for plan administrative functions, it is required to maintain a privacy notice and provide the notice upon request. If the sponsor of a fully insured plan does not have access to PHI, it is not required to maintain or provide a privacy notice.

COMPLIANCE CHECKLIST

To comply with the final HIPAA rule, health plans will need to:

- ☑ Review business associate agreements to determine whether amendments are necessary. Amendments to existing business associate agreements should be made before the end of the transition period. At the latest, this period will end on Sept. 23, 2014, although it may end sooner for some plans.
- ☑ Update HIPAA policies and procedures for the new rule's changes. For example, revisions should be made for the new breach notification standards, expanded individual rights and the prohibition on using genetic information for underwriting purposes.
- ☑ Update workforce training programs for the new requirements. For example, the training should be updated to include information on the risk assessment standard for breach notifications, and the "significant-risk" standard should be replaced with the "low probability" standard.
- ☑ Review the HIPAA privacy notice and make any necessary changes to reflect the final rule. If the health plan has a website, the updated privacy notice should be posted by Sept. 23, 2013. If not, the updated notice should be provided within 60 days of the revision to the notice.

BEACON Specialized Living

Compliance Steps for the Final HIPAA Rule

Employee Name:_____ Date:_____

HIPAA QUIZ 2013

1. T ☐ F ☐ The deadline for compliance on the new HIPAA ruling is September 23, 2013?

2. T ☐ F ☐ Business Associates Agreements are included in this new ruling?

3. T ☐ F ☐ All HIPAA policies need to be updated?

4. T ☐ F ☐ Notice of Privacy Practices need to be revised?

5. T ☐ F ☐ All Electronic devices have to be "password protected"?

6. T ☐ F ☐ A Risk Assessment/Audit for security/safety of protected health information will need to occur at least one time annually?

7. T ☐ F ☐ If a breach is found it does not need to be reported?

8. T ☐ F ☐ PHI stands for Protected Health Insurance?

9. T ☐ F ☐ All contracted entities must have a Business Associates Agreement?

10. T ☐ F ☐ All emails must be encrypted if they contain health related information?