Compliance Alert

Modifications to the HIPAA Privacy and Security Rules Released
Release Date: April 2013

The Department of Health and Human Services (HHS) has issued regulations modifying the Health Insurance Portability and Accountability Act (HIPAA) privacy, security, and enforcement rules. The changes strengthen the privacy and security protection for individual's' health information, modify the rule for breach notifications, and extend HIPAA compliance obligations to additional entities.
Although many of the expanded requirements will be felt most by health care providers and business associates, employers will also be required, at a minimum, to revisit several key areas of their existing HIPAA compliance initiatives. The three areas of the rules with the greatest impact on employers are summarized below.

Background

HIPAA requires covered entities (health care providers, health insurance issuers, group health plans and clearinghouses) to safeguard the privacy and security of individual's protected health information (PHI). HIPAA includes both privacy and security policy and procedure requirements. In 2009, HITECH required that certain of these safeguards be extended to business associates (agents, brokers, TPA's, medical transcriptionist, billing services, etc.) and required breaches of unsecured PHI be reported to individuals and the HHS.

Compliance Effective Date

In general, covered entities must comply with these requirements by September 23, 2013. However there is a delayed effective date specific to changes to business associate agreements (described below) already in place.

Notice of Privacy Practices

Employers must review and may need to revise their existing health plan's notice of privacy practices (NPP) to reflect several changes required by the final rule, including the addition of statements addressing:

- That uses and/or disclosures of psychotherapy notes, PHI for marketing purposes and the sale of PHI will now require authorization from the individual.
- The individual's right to opt out of receiving communications from the covered entity related to fundraising.
- The requirement that the covered entity must agree to an individual's requested restriction on disclosure of PHI if the disclosure pertains solely to a health care item or service for which the individual has paid the covered entity in full (i.e.,paid out of pocket).
- That the covered entity is required to notify affected individuals following a breach of unsecured PHI.

> ***Important note:*** *Many of these changes were first articulated in preliminary guidance released after the passage of HITEC in 2009, so it is possible that existing NPPs have already been updated to reflect the changes contained in the final rule.*

<u>Redistribution of the NPP</u>
Existing HIPAA rules require that an NPP must be redistributed to participants within 60 days after a material change to the notice. In the preamble to the regulations HHS states that these changes are to be considered material changes to the NPP. Depending on how much a particular employer's notice needs to be updated, it may need to be redistributed to plan participants.

A fully insured plan's obligation to provide an NPP depends on whether the plan has access to PHI (other than summary health information and enrollment information).

- If the plan has no access to PHI (other than summary health information and enrollment information), it has no obligation to provide a notice—the notice requirement is imposed solely upon the insurer.
- However, if a fully insured plan has access to PHI (other than summary health information and enrollment information), then the plan must maintain a notice and provide it upon request.(The insurer still has the primary notice obligation.)

Self-funded group health plans must issue their own NPPs.

Distribution of the Notice of Privacy Practices

HIPAA privacy regulations provide covered entities with discretion regarding how to deliver the notice. Special or separate mailings are not required. For example, the covered entity may include the NPP with other written materials that are mailed to the individuals. A plan sponsor may also choose to include the notice with an SPD or with enrollment materials.

The NPP can be provided by email if the recipient has agreed to receive an electronic notice and that agreement has not been withdrawn. However, if the covered entity knows that the email transmission to an individual has failed, the covered entity must provide a paper copy of the notice to the individual. A covered entity that provides its notice to an individual by email may include additional materials in the email, as is the case with a hard-copy mailing.

Redistribution Timing

In general, an updated NPP must be provided by September 23, 2013. However, HHS has clarified that a health plan (including an employer plan sponsor of a health plan) that currently posts its NPP on a website must; prominently post the changes to the NPP by September 23, 2013, provide the revised NPP in the next annual mailing to plan participants, and have printed copies available upon request.

Business Associate Agreements

The final rule expands the definition of business associates to include subcontractors of existing business associates, and makes significant changes extending the direct liability for HIPAA compliance to business associates and their sub-contractors. It also affirms that covered entities are liable for penalties for the failure of a business associate "agent" to perform a function on the covered entity's behalf. As a result, plan sponsors will need to review, and possibly revise, existing business associate agreements.

Employers should make sure that their BA agreements include the following requirements for their business associates:

- Comply with requirements of the HIPAA Privacy Rule applicable to business associates
- Comply with the HIPAA Security Rule with regard to electronic PHI
- Report breaches of unsecured PHI to the covered entity
- Ensure that all subcontractors of the business associate agree to the same restrictions that apply to the business associate

If changes in existing BA agreements are required to be made, and the covered entity and business associate had an agreement in place on January 25, 2013, the parties can rely on the existing agreement until the earlier of either the date such agreement is renewed or modified, or September 22, 2014.

If the parties did not have an agreement in place prior to January 25, 2013, an agreement complying with the requirements of the Final Rule must be in place by September 23, 2013.

Breach Notification

Under the previous Interim Regulations, a breach of unsecured PHI must only be reported if it poses "… a significant risk of financial, reputational, or other harm to the individual." The final rule eliminates this "significant risk of harm" standard. In its place, an impermissible use or disclosure of unsecured PHI is presumed to be a breach requiring notification unless the covered entity can demonstrate through a documented risk assessment that there is a "low probability that the PHI has been compromised."

The risk assessment must consider at least the following four "objective" factors:

- The nature and extent of PHI involved;
- The nature of the recipient that used the PHI or to whom disclosure was made;
- Whether the PHI was actually acquired or viewed (as compared to whether only the opportunity existed for the PHI to be acquired or viewed; and
- The extent to which the breach has been mitigated.

This expanded definition of a breach is likely to increase the frequency with which breaches will occur, thereby increasing the frequency of situations in which notification will be required. As a result, employers that have not already done so may want to revisit the encryption PHI, thereby completely avoiding HITECH's notification requirements.