Security Breach Notification Rules

The 2009 Stimulus Bill imposed new security breach notice requirements. Generally covered entities (group health plans and health care providers) must notify individuals when there is a breach of their unsecured protected health information (PHI). This applies to all kinds of PHI- electronic PHI, PHI on paper and spoken PHI-whether used internally or externally.

The Department of Health and Human Services (HHS) regulations provide that the new rules only apply to "unsecure" PHI. But to be considered secure the PHI must be encrypted or completely destroyed under the standards specified by HHS. Thus, unless a covered entity's PHI is encrypted under these standards or completely destroyed, the PHI will be subject to the security breach notification requirement.

Note covered entities do not have to encrypt data. Entities may rely on firewalls and other access controls. However these controls do not render EPHI secure for the purposes of this rule.

HHS regulations define a breach as a disclosure of unsecure PHI in a manner not permitted under the HIPAA privacy rules that poses a significant risk of financial, reputational or other harm that does not fall under an exception.

Covered entities must perform a fact specific risk assessment to determine if there is a significant risk of harm and thus, if notification is required.

HHS describes 3 exceptions to the breach definition, unintentional access by a covered entity's or business associate's employee in the employee's scope of employment; inadvertent disclosure between employees of a covered entity or a business associate or instances where the recipient would not have been able to retain the PHI.

If there is a breach, covered entities must notify each individual, without unreasonable delay, and in no case longer than 60 days after the breach is discovered. Concurrent notice must be provided to HHS if the breach involved 500 or more individuals, or annually in all other situations.

If the breach involves more than 500 residents in a state, notice must be given to prominent media outlets serving the state. Those outlets may or may not choose to report on the information.

Action: The group health plan will have the ultimate responsibility to ensure that breaches are identified and that any required notifications are provided. However, business associates (e.g., third-party administrators and claims administrators) will often be in the best position to investigate potential breaches and determine if a breach has occurred; whether the harm is significant; and what notification, if any, is required.

The Service Agreement between the group health plan and the business associate should be amended to spell out which party will carry out the investigation, breach determination and the level of control each party will have over the process.

The employer should exam existing plan documents and HIPAA privacy policies and implement any necessary changes to administrative policies and practices to ensure the group health plan can meet the new requirements.