Legal Requirements Triggered by HIPAA Breach

January 26, 2019

An impermissible acquisition, access, use, or disclosure of HIPAA ?ÃÂ£protected health information?ÃÂ¥ (?ÃÂ£***PHI***?ÃÂ¥) under an employer?ÃÃs group health plan (which is a ?ÃÂ£***Covered Entity***?ÃÂ¥ under HIPAA) is not uncommon. If such a breach occurs with respect to the PHI of a Covered Entity, the employer needs to know that the Covered Entity may be required by HIPAA?ÃÃs breach notification rules (the ?ÃÂ£***Breach Rules***?ÃÂ¥) to issue certain notices and perform other tasks. Analysis of the Impermissible Acquisition, Access, Use, or Disclosure of PHI An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a ?ÃÂ£breach?ÃÂ¥ unless the Covered Entity demonstrates that there is a low probability that the PHI has been compromised. The Breach Rules outline the four-factor risk assessment that a Covered Entity must perform (and document) in order to make such a demonstration. If, after completing the step above, the Covered Entity determines that a ?ÃÂ£breach?ÃÂ¥ occurred, the Covered Entity should then confirm whether the PHI involved was ?ÃÂ£unsecured?ÃÂ¥, since only breaches of ?ÃÂ£unsecured?ÃÂ¥ PHI are subject to the notification requirements of the Breach Rules. Under current guidance issued by HHS, there are two methods to ?ÃÂ£secure?ÃÂ¥ PHI: (i) in the case of electronic PHI, by encryption in accordance with HHS?ÃÃs standards and (ii) in the case of non-electronic PHI, by physical destruction. The notification requirements of the Breach Rules will not apply to a breach of PHI that has been ?ÃÂ£secured?ÃÂ¥. Notifications regarding the Breach If the breach involved unsecured PHI, the notification requirements of the Breach Rules are triggered. In that case, the Covered Entity must issue a notification to each individual whose unsecured PHI was involved in the breach (?ÃÂ£***Individual Notice***?ÃÂ¥). The Individual Notice must be issued in accordance with the Breach Rules?ÃÃ delivery specifications no later than 60 calendar days after the breach is discovered. The Individual Notice must contain the information required by the Breach Rules, including (i) a brief description of how and when the breach occurred, (ii) a description of the unsecured PHI that was involved in the breach, and (iii) a description of what the Covered Entity is doing to investigate the breach and mitigate harm to the impacted individuals. Notice of the breach must also be submitted by the Covered Entity to the Secretary of HHS and, depending on the scope of the breach, to media outlets in the jurisdiction of the breach. State Law Requirements In addition, state privacy laws may impose additional reporting and other requirements on employers and/or Covered Entities in the event of a breach of PHI. The employer should determine whether any such state laws apply. Breach-Related Administrative Activities The Covered Entity must maintain for a period of six years the documentation related to its evaluation and administration of the breach, including the risk assessment, the Individual Notices, HHS notice, and any media notices issued. State privacy laws may have different retention periods. Under HIPAA, a Covered Entity must provide, upon request by an individual, an accounting of certain disclosures of the individual?ÃÃs PHI. Such disclosures include impermissible disclosures of an individual?ÃÃs PHI involved in a breach. Accordingly, the Covered Entity should ensure that breach-related disclosures are logged for such purposes.