September 23 Deadline for HIPAA Omnibus Rule Compliance

09.13.2013

BY: PATRICK C. DEVINE, JR.

Introduction. Significant modifications were made to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules by a final rule (the "HIPAA Omnibus Rule") issued by the Department of Health and Human Services ("HHS") on January 25, 2013. Covered entities (like providers, health plans, and clearinghouses) and business associates must comply with these changes by September 23, 2013. To ensure compliance, changes likely will need to be made to each covered entity's and business associate's privacy policies, security policies, business associate agreement forms and training protocols.

Changes. Among the changes imposed by the Omnibus Rule are: (i) strengthened limitations on the use or disclosure of PHI to facilitate fund raising and marketing, (ii) new and more objective obligations for breach notification, (iii) prohibition on the sale of PHI without the affected individual's permission, (iv) expanded patient rights to receive electronic copies of PHI, (v) restrictions on disclosures to health plans where the patient has fully paid for all out-of-pocket expenses related to the particular item or service, (vi) restrictions on health plans' use of genetic information for underwriting, (vii) greater flexibility for the disclosure of immunization records, and (viii) an increased and tiered civil money penalty structure for violations.

Business Associates. The new rules make Business Associates directly liable for compliance with certain HIPAA Privacy and Security Rule requirements. If a compliant Business Associate Agreement was in effect on March 26, 2013, it does not need to be updated to comply with the Omnibus Rule until September 22, 2014, unless it was modified or expired in the interim. The new requirements for Business Associate Agreements include: (i) confirmation of direct liability for the business associate, (ii) a requirement that the business associate enter into similar agreements with any subcontractor or third party to whom the business associate provides PHI to facilitate the business associate's obligations to the covered entity, and (iii) compliance with new breach notification rules.

Training and Liability. In addition to updating policies that facilitate compliance, it is also important that covered entities and business associates implement training programs for their personnel to ensure that compliance with the Privacy and Security Rules is achieved and documented. Importantly, the tiered policy for liability for a covered entity or a business associate turns, in large measure, on whether a violation was without knowledge or was a result of willful neglect.

Conclusion. To the extent a covered entity or potential business associate has not yet updated its policies and agreements to comply with the HIPAA Omnibus Rule, it is important to evaluate its existing

policies and agreements and to take affirmative steps to ensure compliance by the deadline. Should you have any questions concerning the HIPAA Omnibus Rule, please feel free to call Pat Devine at 757-629-0717 (pdevine@williamsmullen.com) or call any other member of the Williams Mullen Health Care Team.

Related People

- Patrick C. Devine, Jr. – 757.629.0614 – pdevine@williamsmullen.com

Related Services

- Health Care