HHS Issues Notification Requirements for Breaches of Protected Health Information

On August 24, 2009, the Federal Register published a Department of Health and Human Services (HHS) interim final rule implementing new breach notification requirements for unsecured protected health information (PHI). The interim final rule requires providers, health plans, and other covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to notify affected individuals, the Secretary of HHS and, in certain circumstances, the media of breaches of unsecured PHI. HHS also issued further guidance regarding technologies and methodologies that render PHI secured, such that disclosure of secured information will not trigger a notification requirement. Covered entities and business associates should implement procedures for proper assessment and, if required, notifications in the event breaches of unsecured PHI occur. Moreover, business associate agreements may need to be updated to require business associates to inform covered entities of breaches of unsecured PHI.

The rule implements provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery and Reinvestment Act of 2009. HHS developed the rule in consultation with the Federal Trade Commission (FTC), which has issued companion breach notification regulations applicable to vendors of personal health records and other entities not subject to HIPAA. HHS is accepting public comments until October 23, 2009.

Scope of the Breach Notification Requirements

The breach notification requirements are triggered only when there is a breach of unsecured PHI. The interim final rule defines the terms "unsecured protected health information" and "breach."

Unsecured Protected Health Information. In the preamble, HHS updated guidance issued on April 17, 2009 specifying technologies and methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals. Electronic PHI has been secured if it has been encrypted and the decryption process or key has not been breached. PHI in a hard-copy format, such as paper, has been secured if it has been shredded or destroyed so that the PHI is unreadable and otherwise cannot be reconstructed. The rule specifies that redaction is an insufficient means of securing data. PHI protected through other means, even means that comply with the HIPAA Security Rule, is considered unsecured for purposes of the breach notification requirements.

Breach. The interim final rule clarifies that a breach only occurs when the acquisition, access, use or disclosure of PHI violates HIPAA's Privacy Rule and compromises the security or privacy of the PHI. Consistent with many state breach notification laws, such an act "compromises the security or privacy of the protected health information" if it "poses a significant risk of financial, reputational, or other harm to the individual." To determine whether the risk of harm is significant, covered entities and business associates will need to conduct a risk assessment that considers a combination of factors set forth in the rule.

The interim final rule also sets forth exceptions in which an unauthorized acquisition, access, use or disclosure of PHI will not be considered a breach. The exceptions apply to any unintentional or inadvertent acquisition, access, use or disclosure of PHI by a workforce member, person who is acting under the authority of a covered entity or business associate, or person authorized to access PHI as a covered entity or business associate, which cannot result in any further use or disclosure not

otherwise permitted by the HIPAA Privacy Rule. Another exception applies to disclosures where the disclosing covered entity has a good faith belief that such information would not reasonably have been able to be retained by the recipient.

Accordingly, a breach has occurred if: (1) there has been a violation of the Privacy Rule; (2) the violation poses a significant risk of financial, reputational or other harm to the individual; and (3) no exception applies.

Notifications to Individuals, Media and Secretary of HHS

The interim final rule describes the breach notifications covered entities must provide to affected individuals, the Secretary of HHS and, in certain circumstances, to the media. Business associates are required to notify covered entities following the discovery of a breach of unsecured PHI. If a business associate is acting as an agent of a covered entity, the business associate's discovery of the breach will be imputed to the covered entity and the obligation to provide notice runs from the date of discovery by the business associate. As a result, business associate agreements will need to be reviewed and amended to ensure compliance with the notification standard.

Notifications to Individuals. After discovery of a breach of unsecured PHI, a covered entity must "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach." Knowledge of a breach is attributed to the covered entity if certain individuals, including agents, have knowledge, or by exercising reasonable diligence would have had knowledge, of the breach. Accordingly, covered entities are advised to implement appropriate systems for the discovery of breaches. Individuals must be notified without unreasonable delay and within 60 days of discovery, and the notification must contain specified elements. The rule adopts the statutory provisions for actual written notice to the affected individuals by first-class mail and substitute notice to individuals if their contact information is insufficient or out-of-date. The form of substitute notice depends on the number of affected individuals for whom the covered entity has insufficient or out-of-date information.

Notifications to the Media. Covered entities are required to provide notice to prominent media outlets following the discovery of a breach of unsecured PHI involving more than 500 individuals of any one state or jurisdiction. This notice must also be made within 60 days of discovery.

Notifications to the Secretary. Notice must also be provided to the Secretary, either concurrently with the notification to each individual (in the case of a breach involving 500 or more individuals) or on an annual basis not later than 60 days after the end of each calendar year (in the case of a breach involving fewer than 500 individuals). The names of covered entities that submit reports of breaches of unsecured PHI involving more than 500 individuals to the Secretary will be posted on the HHS Web site.

The rule also provides for a delay in notification in the event a law enforcement official indicates to a covered entity or business associate that notification "would impede a criminal investigation or cause damage to national security."

Effective Date and Sanctions

The rule is effective and compliance is required for breaches occurring on or after September 23, 2009. The Office of Civil Rights will not, however, impose sanctions for failure to satisfy the notification requirements for breaches discovered before February 22, 2010.

If you would like to learn more about the issues raised by this update, please contact your usual Ropes & Gray attorney.