January 2013

A Detailed Analysis of Changes to HIPAA and the Implications for Healthcare Providers and Others in the Healthcare Industry

On Friday, January 25, 2013, the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") published a final rule modifying the HIPAA Privacy, Security, and Enforcement Rules (the "Final Rule") as mandated by the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Many of these modifications were set forth in a Notice of Proposed Rulemaking ("NPRM") dated July 14, 2010, although the Final Rule does not adopt all the proposals as described in the NPRM.

The Final Rule also modifies the Breach Notification Rule, which has been effective as an interim final rule since September 23, 2009. Finally, the Final Rule strengthens privacy protections for certain genetic information under the Genetic Information Nondiscrimination Act ("GINA").

The Final Rule makes significant changes to HIPAA and the potential penalties for violating HIPAA. The Final Rule also expands the scope of HIPAA, meaning that some businesses that were not subject to HIPAA before the Final Rule now have HIPAA compliance obligations and can be subject to enforcement action for noncompliance. Healthcare providers and others in the healthcare industry should be aware of these changes and how they will apply to their particular business.

The Final Rule is effective on March 26, 2013, and Covered Entities and Business Associates must comply with the Final Rule by September 23, 2013.

Changes to the HIPAA Breach Notification Rule

Background: The HITECH Act required Covered Entities to notify individuals, HHS, and in some cases, the media, of a Breach of Unsecured PHI. A Business Associate is required to notify the Covered Entity of any such Breaches so that the Covered Entity may make the notifications listed above. In response to the HITECH Act, OCR issued an interim final Breach Notification Rule effective on September 23, 2009 incorporating the requirements of the HITECH Act.

In the interim final Breach Notification Rule, a Breach was defined as, subject to certain exceptions, the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom the information is disclosed would not reasonably have been able to retain such information. An unauthorized acquisition, access, use, or disclosure of PHI compromised the security or privacy of the PHI if it posed a significant risk of financial, reputational, or other harm to the individual. In other words, to determine if a Breach occurred as a result of an impermissible use or disclosure of PHI, a Covered Entity was required to perform a risk assessment to determine if there was a significant risk of harm to the individual.

Unsecured PHI was defined as PHI not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS in guidance. The guidance on securing PHI published by HHS on April 27, 2009 listed encryption and destruction as the two technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Modifications: While many provisions of the interim final Breach Notification Rule are not amended by the Final Rule, the Final Rule does make a significant change by amending the definition of Breach. Instead of using the "risk of harm" standard provided in the interim final Breach Notification Rule to determine when a Breach has occurred, the Final Rule provides that any acquisition, access, use, or disclosure of PHI not permitted by the Privacy Rule is presumed to be Breach of Unsecured PHI unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised.

To determine whether there is a low probability that the PHI has been comprised, the Covered Entity or Business Associate must complete a risk assessment taking into account the following four factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated. Covered Entities and Business Associates should move quickly to update their Breach Notification policies and procedures to ensure that risk assessments address these factors.

OCR reaffirms in the Final Rule that if PHI is encrypted pursuant to guidance issued by OCR, it is not "Unsecured" and therefore no notification is required following an impermissible use or disclosure of the PHI.

If you have any questions about the Final Rule or HIPAA please contact Jill M. Girardeau, the principal drafter of this alert, Sarah B. Crotts, Deonys de Cárdenas, Tracy Field, or any member of Womble Carlyle's Healthcare Industry Team.