OCR Releases Final HIPAA Regulations

January 18, 2013

The Office of Civil Rights has released the text of the long-anticipated final Health Insurance Portability and Accountability Act ("HIPAA") regulations, which are scheduled to be published in the federal register on January 25, 2013. The regulations are effective on March 26, 2013, providing covered entities and business associates until September 23, 2013 to comply.

Breach Notification

One of the highly anticipated provisions in the final regulations relates to breach notification. This final rule replaces the interim rule for HIPAA breach notification, originally published on August 24, 2009. Under the 2009 rule, a "breach" only included those impermissible uses or disclosures of protected health information that posed a significant risk of financial, reputational, or other harm to the individual. This was often referred to as the "risk of harm" threshold. The final rule removes the risk of harm threshold from the definition of a breach.

Under the new rules, an impermissible use or disclosure of protected health information is presumed to be a "breach" unless the covered entity demonstrates there is a low probability that the protected health information has been compromised. This demonstration is accomplished through a risk assessment demonstrating that there is low risk that the information has been compromised.

The risk assessment must consider the following four factors: 1) the nature and extent of protected health information involved, including the types of identifiers and likelihood of re-identification; 2) the unauthorized person who used the protected health information or to whom the disclosure was made; 3) whether the protected health information was actually acquired or viewed; and 4) the extent to which the risk to the protected health information has been mitigated. If the risk assessment fails to demonstrate there is low probability that the information has been compromised, breach notification to the individual, HHS, and, in some circumstances, media is required.

HIPAA Privacy and Security Changes

The final regulations also implement numerous additional changes to HIPAA required under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Of greatest significance is the

direct application of HIPAA Privacy and Security requirements to business associates. Under these changes, the HIPAA Privacy and Security regulations and associated penalties apply to business associates as if they were covered entities.

Additionally, the final HIPAA regulations modify several definitions including minimum necessary, marketing, electronic media, and business associate. They require revision of notice of privacy practices and business associate agreements in addition to policies and procedures. The regulations implement the new penalty structure established under HITECH and provide clarification of the levels of intent and factors to be considered by OCR when assessing penalties.

Expectations of Covered Entities and Business Associates

The publication of these final regulations has started the clock on compliance for covered entities and business associates. It is necessary for these organizations to:

- Implement or revise policies and procedures;
- Update their notice of privacy practices;
- Amend business associate agreements; and
- Modify the manner in which they determine whether breach notification is required.

Watch for future client alerts from Lathrop Gage discussing detailed requirements under these regulations.