HIPAA Final Rule Compliance

On January 17, 2013, the Department of Health and Human Services released a Final Rule implementing significant changes to the HIPAA Rules. The Final Rule accepted without change many requirements proposed in the Breach Notification Interim Final Rule, which apply to breaches occurring after September 22, 2009, and in the Enforcement Interim Final Rule, which apply to violations occurring after February 17, 2009.

The Final Rule also modified several provisions in the Privacy, Security, and related rules. Covered entities and business associates must be in compliance with most of these modifications by September 23, 2013; new requirements for certain Business Associate Agreements, discussed below, are applicable as of September 23, 2014. In preparation for the compliance deadline, covered entities and business associates should review and update their policies and procedures and provide workforce training on any new or revised policies. Significant changes in the Final Rule include:

New Breach Standard
The Final Rule created a new standard for determining when a breach of unsecured protected health information occurs, which presumes a breach occurred unless a risk assessment conducted by the covered entity or business associate shows a low probability that information was compromised, replacing the original "risk of harm" standard. Covered entities and business associates must implement a HIPAA-compliant risk assessment process.

Expanded Definition of Business Associates
The Final Rule re-defined "business associates" to include subcontractors and certain types of data transmission providers and patient health record vendors. Covered entities and business associates should review all service provider and vendor relationships and ensure that a HIPAA-compliant business associate agreement is in place with all "first tier" business associates. Business associate agreements entered into before January 26, 2013 that have not been modified since March 26, 2013 do not have to be updated until September 23, 2014.

Privacy and Security Rule Modifications
The Final Rule changed several provisions of the Privacy and Security Rules, including new limitations on marketing, fundraising, and sale of protected health information, increased flexibility for disclosure of decedents' information, and reduced time to respond to patient records requests. Many changes enhance patients' rights, including the right to receive an electronic copy of records and increased ability to limit certain disclosures. Finally, revisions to the content that must be included in Notices of Privacy Practices require covered entities to update and re-distribute their Notices in conformance with HIPAA requirements.

Enforcement Rule Changes
The Final Rule requires HHS to investigate certain complaints and impose civil monetary penalties. Business associates are now subject to direct liability for privacy, security, and breach notification violations and covered entities and business associates are subject to vicarious liability when their agents violate HIPAA requirements.

For more information about HIPAA, see www.healthinfolaw.org/federal-law/HIPAA.
For resources on business associates, see www.healthinfolaw.org/announcement/hipaa-BA-resources.
Follow us on Twitter at **@HealthInfoLaw**