THOMPSON COBURN LLP

2013 HIPAA Changes

On January 17, 2013, the Department of Health and Human Services issued the long-awaited revisions to the HIPAA rules, making a number of changes to the current HIPAA privacy, security, breach notification and enforcement requirements. The major provisions of the new rules are briefly addressed below.

• The new rules adopt an increased, tiered civil money penalty structure for HIPAA violations provided by the HITECH Act. They also give the Office of Civil Rights discretion to impose penalties on covered entities and business associates in cases of violations due to willful neglect, instead of first attempting to resolve the matter through informal means. Penalties for HIPAA violations are significant. Specifically, penalties for violations caused by willful neglect, which are corrected, range from $10,000 to $50,000 per violation. The minimum penalty for an uncorrected HIPAA violation caused by willful neglect is $50,000 per violation. The penalties are capped at $1.5 million for all violations of an identical requirement in a calendar year.

• The new rules change the notification requirements for breaches of unsecured protected health information ("PHI") by replacing a current "risk of harm to the affected patients" standard with a more objective standard to be used in determining whether a breach has occurred and whether notice of the breach must be provided to patients, the government and the media. Under the new rules, every improper use or disclosure of PHI is presumed to be a breach unless it is

demonstrated that there is low probability that the PHI was compromised as a result of the incident. This change is significant and could result in an increase in the number of breaches requiring notice.

• The definition of the term "business associate" has been expanded in the new rules to include vendors who maintain PHI, even if they do not view the PHI, and subcontractors of business associates. This change to the rules will likely result in many new vendors being considered business associates.

• The new rules make clear that business associates, as well as the subcontractors of business associates, are directly liable for compliance with the HIPAA security rules and certain requirements of the HIPAA privacy rules. They also require amendment of business associate agreements to address certain requirements of the new rules. While business associate agreements already revised for compliance with the HITECH Act may not require a significant overhaul, most business associate agreements will likely require some revisions to track the requirements of the new rules.

• The new rules impose additional restrictions on the use and disclosure of PHI for marketing by requiring written patient authorization for all communications in cases where a covered entity receives remuneration for making the communication from a third party whose product or service is being marketed, even if the communication is for treatment-related purposes.

• The new rules modify the patient authorization and other requirements related to use and disclosure of PHI for research.

• Consistent with the Genetic Information Nondiscrimination Act, the new rules prohibit most health plans from using or disclosing genetic information for underwriting purposes.

• The new rules provide more flexibility with respect to allowing access to decedent PHI to family members and others.

• Consistent with the provisions of the HITECH Act, the new rules expand patients' rights to receive electronic copies of their PHI and restrict disclosures of PHI to health plans concerning treatment for which the patient paid out of pocket in full.

• The new rules provide that each covered entity must revise its notice of privacy practices to address the new HIPAA requirements.

Covered entities and business associates generally must comply with the new HIPAA requirements by September 23, 2013. Compliance with the new requirements will require changes to HIPAA policies and procedures, modifications to business associate agreements and revisions to notices of privacy practices. If you have any questions about the new HIPAA requirements or would like any assistance with revising your HIPAA documents, please contact your Thompson Coburn attorney, or any of the attorneys in our Healthcare practice.

Allen D. Allred	314-552-6001	aallred@thompsoncoburn.com
Don L. Daniel	314-552-6379	ddaniel@thompsoncoburn.com
James L. Fogle	314-552-6035	jfogle@thompsoncoburn.com
Kelly L. Gawne	312-580-2224	kgawne@thompsoncoburn.com
Evan Raskas Goldfarb	314-552-6198	egoldfarb@thompsoncoburn.com
A. Jay Goldstein	312-580-2207	agoldstein@thompsoncoburn.com
Milada R. Goturi	202-585-6951	mgoturi@thompsoncoburn.com
James F. Gunn	314-552-6189	jgunn@thompsoncoburn.com
Joyce Harris Hennessy	314-552-6165	jhennessy@thompsoncoburn.com
Robert N. Kamensky	312-580-2247	rkamensky@thompsoncoburn.com
Richard J. Lang	312-580-2220	rlang@thompsoncoburn.com
Joan M. Lebow	312-580-2212	jlebow@thompsoncoburn.com
Jan Paul Miller	314-552-6365	jmiller@thompsoncoburn.com
Suzanne E. Ritzler	312-580-2227	sritzler@thompsoncoburn.com
Claire M. Schenk	314-552-6462	cschenk@thompsoncoburn.com

Thompson Coburn LLP
Chicago | St. Louis | Southern Illinois | Washington, D.C.
www.thompsoncoburn.com

This newsletter is intended for information only and should not be considered legal advice. If you desire legal advice for a particular situation you should consult an attorney. The ethical rules of some states require us to identify this as attorney advertising material. The choice of a lawyer is an important decision and should not be based solely upon advertisements.