LEGAL BRIEFING: HIPAA
Compliance Deadline of September 23, 2013 Approaching

August 14, 2013

On August 14, 2013, the United States Department of Health and Human Services announced that it reached a settlement with Affinity Health Plan, Inc. (a New York not-for-profit managed care plan) for potential violations of HIPAA – amounting to $1,215,780 in fines to be paid by Affinity. This fine was prompted by Affinity's own self-disclosure and compliance with the HIPAA Breach Notification Rule, which requires HIPAA covered entities (including health care providers and health plans) to notify the government and individuals when there is a breach of unsecured protected health information.

In the case of Affinity, the government reported that Affinity had been informed in 2010 by CBS Evening News that as part of an investigation it had purchased a photocopier previously leased to Affinity and that the photocopier that Affinity had used still contained confidential medical information used by Affinity on its hard drive. Affinity had returned numerous photocopiers to leasing agents without first erasing the data on the copier hard drives and had also failed to incorporate the electronic protected health information stored on its photocopier hard drives as part of its HIPAA Security Rules compliance program.

The enormous fine in this case illustrates how significant it is for HIPAA covered entities – health care providers, health plans, and health care clearinghouses – to make sure that they have robust HIPAA compliance plans in place. This compliance obligation is especially relevant now in light of the upcoming September 23, 2013 compliance date when a significant number of changes to the HIPAA regulations take effect.

The Affinity case also red flags how health information may be stored where you least expect it – in photocopiers and electronic devices other than just your computers. It is crucial that covered entities revisit their HIPAA Security Rules compliance plans to make sure they address this issue in their Security Rules Disposal and other applicable safeguard policies. The HIPAA Security Rules were effective in 2005 and only apply to electronic protected health information.

Covered entities should have a HIPAA Security Rules compliance plan in place with written policies and procedures to address each of the 18 Administrative, Physical, and Technical Safeguards and their accompanying 35+ implementation specifications, as well as other accompanying policies to address issues such as the safeguarding of information sent by facsimile.

The written HIPAA Security Rules compliance plan should be in addition to the written HIPAA Privacy Rules compliance plan which addresses issues such as access to protected health information and the requirement to issue patients a Privacy Notice/Notice of Privacy Practices.

With respect to the September 23, 2013 compliance date, HIPAA covered entities must ensure that they address the following issues:

- Most Business Associate Agreements will need to be updated to address changes to both the Privacy and Security Rules. Most significantly, Business Associates are now directly liable for non-compliance with portions of the HIPAA Rules. Also, Business Associates must ensure compliance by their own subcontractors by entering into "Subcontractor" Business Associate Agreements.

- Health Care Providers and Health Plans must modify and redistribute their Privacy Notices/Notices of Privacy Practices to address a number of new requirements.

- The HIPAA Breach Notification requirements, which were at issue in the Affinity case example noted above, have been modified significantly by replacing the "harm" threshold for breach notification with a more objective standard in which breach notification is necessary unless there is a showing that there is a "low probability" that the health information has been compromised.

- The penalties for violations of the HIPAA Rules have been greatly enhanced, which in some cases may reach $1.5 million per violation, as reflected in the Affinity case example noted above.

- Patients have new rights – the ability to receive electronic copies of their health information and the ability to request restrictions on the disclosures to a health plan concerning treatment for which the patient has paid in full out of pocket.

These examples are only a sampling of the changes made to the HIPAA Rules that need to be addressed by September 23, 2013.

If you have any questions about any of these compliance requirements or the steps your organization needs to take by September 23, 2013, please contact any attorney of our Firm at 585-730-4773.