2013 HIPAA OMNIBUS RULE

The U.S. Department of Health & Human Services' (HHS') issuance of the final Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule ("Rule") in March completed the revamping of the HIPAA regulations that began with the implementation of the Health Information Technology for Economic and Clinical Health Act (HITECH) back in 2010. Keenan previously addressed the HITECH changes in our November 2009 Briefing. This Briefing will address some of the most significant changes ushered in by the Rule.

Among the most significant change is that Business Associates (BAs) are now regulated under the HIPAA Privacy and Security Rules. This means that they, like Covered Entities*, are directly accountable to HHS. Previously, a BA's only HIPAA obligations were contractual under the terms of its Business Associate Agreement (BAA) with a Covered Entity client.

The definition of BA has been expanded to include entities that maintain or store protected health information (PHI). In addition to storage facilities and records management companies where paper files may be kept, the expanded definition also includes the high-tech vendors offering cloud storage capabilities.

Also new is the requirement that any subcontractor engaged by a BA must execute a BAA if it will be accessing or using the PHI of the BA's clients. Although this is a new requirement under the Rule, it has long been Keenan's organizational practice to obtain BAA's from all such subcontractors.

Health care providers are now permitted to provide, without a formal written authorization, proof of a student's immunization to a school if state law requires proof of immunization prior to admission. The provider must, however, obtain at least a verbal consent from the parent, guardian or individual (if over 18 or an emancipated minor) prior to making the disclosure.

While the breach notification rules are not new – and were addressed in our 2009 *Briefing* – the Rule does contain some important changes. The definition of breach has been updated so that the unauthorized use or disclosure of unprotected PHI is now presumed to be a breach unless a formal risk assessment (RA) demonstrates otherwise. Four factors must be considered when performing a RA:

i) Nature and extent of information disclosed;

ii) The person(s) who accessed or acquired the PHI;

iii) Whether or not the PHI was in fact accessed or viewed; and

iv) The extent to which the risk of harm to the individual has been mitigated. If the RA shows that there is a low probability that the PHI has been compromised, then the disclosure is not considered a reportable breach.

* Covered Entities include, among other things, health care providers and health plans. The latter may be medical, dental, vision, pharmacy, EAPs or Section 125 plans. Both fully insured and self-funded health plans are subject to HIPAA.

Violations of the "minimum necessary" rule are also considered potential breaches and must be treated as such. A proper RA must be done to prove that the violation was not a breach. Under the minimum necessary rule one may disclose only the least amount of information necessary to accomplish the purpose of the disclosure. For example, if someone is to audit all third party administrator (TPA) files for medical claims processed in *July* 2012 but receives a folder containing information on all claims for *calendar year* 2012, a violation of the "minimum necessary" rule has occurred. That is, more information than was needed (or requested) was provided.

If requested, a patient may now receive a copy of his/her medical records in electronic form. An individual may also restrict disclosure of certain PHI to a health plan if the PHI relates to medical treatments, procedures, or medications for which that person has elected to pay out of pocket rather than submitting the claim through the plan.

Tighter controls have been placed on using PHI for fundraising and on the use of PHI for marketing. PHI may not be sold without the written authorization of the individual whose information is being sold.

Covered entities must update their notices of privacy practices to reflect the new changes and BAAs must likewise be updated. Keenan is in the process of sending out updated BAAs to the appropriate account contacts now. If your organization has not received a BAA by September 15, 2013 please let your account representative know.

The Rule has adopted the penalty structure introduced by HITECH. Penalties can range from $100 to more than $50,000 per violation with a maximum annual penalty of $1.5 million. The annual aggregate $1.5 million applies to a single type of violation. A non-compliant entity with several different types of violations can easily find itself facing penalties totaling far more than the $1.5 million aggregate.

Although not part of the Rule, it is important to mention that the pilot audit program conducted last year by HHS will be implemented as a formal program in 2014. Both Covered Entities and BAs now face the possibility that their HIPAA compliance programs may be subject to random audits by HHS.

The Rule comprises over 500 pages and what is presented here barely skims the surface. While Keenan does not provide extensive HIPAA consulting services, we nonetheless wanted to call your attention to this important development. More information can be obtained through the links below. Your legal advisor can provide a more in-depth analysis of the Rule and its application to a particular situation.

http://www.sidley.com/the-omnibus-hipaa-rule-a-new-era-of-federal-privacy-regulation-02-07-2013/
http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php
www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

For additional questions regarding this topic, please contact your Keenan Account Representative.