Highlights From Leon Rodriguez, Executive Director of OCR's, Speech at ABA's EMI Conference in Miami – February 22, 2013

- The biggest change to HIPAA is how business associates are regulated, and who are business associates
    - When going through findings from OCR's HIPAA audits, investigations, and breaches that have been reported, Leon emphasized that 60% of the breaches are coming from business associates, and that there is a desire to put BA's skin in the game
- Biggest finding from audits is that there is no Security Rule Risk Assessment
- Leon's Beliefs re: the Changed Breach Notification Rule:
    - There is and has been a significant underreporting of breaches
        - BUT
    - For 98% of the providers out there who are doing things correctly, the breach/no-breach outcome, and their decision trees for reaching the same, will not be significantly impacted by the final HIPAA Megarule
        - *[ED: This confirms the analysis that HLP attorneys have promulgated, which is that the breach rule changes are not as significant as they were initially reported, see, e.g., http://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1301_hipaa_mikel.html]*
    - In most cases, the decisional factors are going to work the same way. Flipped the presumption, but still have the risk assessment element.
- In OCR's HIPAA enforcement work, it's like a high school math test. They are looking for you to show the work and the process, and they will not give heavy-handed enforcement to those that gave good faith efforts to follow the process. Answer/outcome is not always correct, but process is important.
- Leon thinks that most cases/penalties will fall into the two higher tiers of penalties

Violation Category	Each Violation	Total CMP for Violations of an Identical Provision in a Calendar Year
Unknowing	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	At least $50,000	$1,500,000

- Indicates that nearly everyone who has done a risk assessment, has determined that they should encrypt because the cost is low and the benefits are high. The ones who did not encrypt are those that did not think about it at all. *[ED: Another indicator that OCR is nearly de facto considering encryption to be a required implementation specification]*
- OCR Is Giving Guidance
    - Guidance coming out soon for patients on their HIPAA rights
    - Guidance coming out soon re: minimum necessary
    - New series of Medscape CME videos for CE's
- OCR's budget has decreased, but their regulated entities has increased
    - Thus, their enforcement is moving to a more IMPACT focused model, to deter systemic violations
- Covered entities are pleased by the additional new business associates who are directly regulated, and OCR has NOT yet received significant pushback from the new business associate community

For more information, please contact Adrienne Dresevic, Esq. or Clinton Mikel, Esq. at (248) 996-8510 or visit The HLP Webiste.