eALERT

INCompliance

January 15, 2013

OCR's First-Ever Settlement for a Breach Affecting Fewer Than 500 People

The Health and Human Services' Office for Civil Rights has entered a first-ever settlement for a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals. The settlement agreement — $50,000 to be paid to OCR, and a strict reporting obligation of future breaches — illustrates the new lengths to which the federal government is willing to pursue violators of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The violation was two-fold. The provider failed to (1) evaluate the confidentiality risks to its portable devices, nor did it implement, document or maintain proper security measures to address such potential risks; and (2) the provider failed to adopt or implement security measures sufficient to ensure the confidentiality of ePHI to a reasonable and appropriate level.

OCR's investigation was prompted when the provider, the Hospice of North Idaho (HONI), reported the theft of an unencrypted laptop computer containing the ePHI of 441 patients. It is what the OCR discovered upon investigating the theft that created the $50,000 problem for HONI, placing the rest of the country on notice.

"This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information," OCR Director Leon Rodriguez said in a press release.

In addition to the financial settlement, HONI also agreed to a two-year obligation of notifying OCR in writing within 30 days of discovering that a workforce member may have failed to comply with privacy and security policies and procedures. The reports must include a complete description of the event, a description of the actions taken and any further steps HONI might plan to take in addressing the matter in mitigating harm and preventing a recurrence.

Practical Tip: All covered entities should review their current policies and procedures and security risk assessments to see if they are current and effective. 2013 would be a good year for a self-assessment audit of HIPAA privacy and security requirements.

This eAlert was prepared by Karen Smith (614) 227-2313 or ksmith@incomplianceconsulting.com and Michael Corey (614) 227-4867. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com.