# PUBLICATION

## First OCR Settlement Involving a "Small" Breach Focuses on Mobile Device Security

**2013: Issue 1**

**In what is best understood as a follow-up to both the recent settlement with MEEI and the release of its mobile device security guidance, HHS OCR recently released details of a settlement reached with the Hospice of Northern Idaho (HONI) that again focuses on the entity's failure to properly secure mobile technology containing protected health information (PHI). HONI will pay a $50,000 fine and has entered into a two-year Corrective Action Plan (CAP) that notably does *not* include provisions for independent monitoring of HONI's compliance activities.**

OCR's investigation of HONI began in July 2011, about six months after OCR received HONI's notification that a laptop had been stolen containing the PHI of 441 patients. OCR's press release notes that the use of a laptop itself was not surprising since “[l]aptops containing ePHI are regularly used by the organization as part of their field work.” While neither OCR's press release nor the Settlement Agreement detail the investigation, the date of the settlement agreement (signed December 17, 2012) indicates that it extended beyond a cursory review of HONI's written policies and procedures. In pertinent part, the Settlement Agreement notes that HONI failed to meet the standards of the Privacy and Security Rules in two ways:

(A) HONI did not conduct an accurate and thorough analysis of the risk to the confidentiality of ePHI on an on-going basis as part of its security management process from the compliance date of the Security Rule to January 17, 2012. In particular, HONI did not evaluate the likelihood and impact of potential risks to the confidentiality of electronic PHI maintained in and transmitted using portable devices, implement appropriate security measures to address such potential risks, document the chosen security measures and the rationale for adopting those measures, and maintain on an on-going basis reasonable and appropriate security measures.

(B) HONI did not adequately adopt or implement security measures sufficient to ensure the confidentiality of ePHI that it created, maintained, and transmitted using portable devices to a reasonable and appropriate level from the compliance date of the Security Rule to May 1, 2011.

Notably, both failures hinge on HONI's treatment of portable electronic devices; specifically, its failure to address the unique risks posed by mobile electronic devices and to provide policies and procedures designed to account for and address those risks. This focus should not come as a surprise to those who follow OCR enforcement activity, but it is an important reminder that enforcement activities are not limited to large breaches.

## Comments

Several recent issuances by OCR have focused on mobile device security and providers should follow this emphasis in their risk analysis and policies and procedures. A significant number of the data breaches reported to OCR each year arise from lost or stolen mobile devices. At a minimum, covered entities and business associates should perform a risk assessment with particular regard to their mobile devices and their use and review their existing policies and procedures governing the use of mobile devices to access and store PHI.

Providers who use mobile devices should also familiarize themselves with the guidance OCR recently released on the subject and take recommended steps.