HHS Announces First Settlement Of Small-Scale HIPAA Breach

01.25.2013

BY: BRIAN C. VICK

Continuing its streak of HIPAA enforcement actions over the past year, the United States Department of Health and Human Services? Office of Civil Rights (?OCR?) recently announced a $50,000 settlement with Hospice of North Idaho (?HONI?) arising from the theft of a laptop that contained unencrypted patient data. Although the amount of this resolution is modest in relation to other recent enforcement actions, and the circumstances of the breach (i.e., stolen mobile device) are no longer novel, this settlement has two important lessons for any entity that deals with electronic protected health information (?ePHI?).

1. The size of a breach does not matter.

In contrast to recent high-profile enforcement actions by OCR that involved data on as many as 1 million individuals, HONI?s breach involved the ePHI of only 441 individuals and, therefore, did not trigger the provisions of the HITECH Act that require prompt notification of a breach. Instead, HONI was simply required to notify OCR of the breach, which occurred in 2010, as part of its annual reporting obligations under HITECH. In settling with HONI in such a public fashion, OCR made a clear pronouncement that small-scale breaches put an entity at just as much risk of an investigation and enforcement action as the larger-scale breaches that it has highlighted in the recent past. As a result, any entity that experiences a breach of any size ? particularly one involving ePHI ? should respond immediately and proactively. At a minimum, this response should involve a thorough risk analysis and appropriate mitigation efforts to ensure that all existing data security risks have been identified and addressed.

2. Mobile device security cannot be ignored.

As with several other recent high-profile enforcement actions, the breach that led to the action against HONI had its origins in lax organizational oversight of mobile devices. Although employees of HONI routinely used laptops in their work, HONI had not taken appropriate steps to ensure the security of the data on those devices, a failure that OCR highlighted in its announcement of the settlement. Specifically, OCR noted that HONI had not adopted policies and procedures to address mobile device security and had not conducted an appropriate risk analysis to safeguard its ePHI. Given the prevalence of mobile device use in the health care sector and the ease with which such devices can be lost or stolen, it is critically important for any entity dealing with ePHI to ensure that it has a clear understanding of how mobile devices are being used within its organization and that such use does not risk unauthorized disclosure of ePHI. Notably, OCR used the HONI settlement to stress once again that entities can mitigate a substantial amount of the risk emanating from mobile device use by encrypting any ePHI that resides on those devices.

For anyone who has followed OCR?s HIPAA enforcement actions over the past year, the HONI settlement serves as further confirmation that this enforcement campaign is not temporary and, instead, represents the new regulatory norm. Thus, any entity that deals with ePHI would be well advised to make sure that its HIPAA compliance efforts are in line with the requirements that OCR has telegraphed through the various settlements announced over the past year. Now is a particularly opportune time to review such compliance efforts given the changes in HIPAA that HHS has just announced will take effect in March 2013.

Related People

Related Services

- Health Care
- Health Care Litigation