Published on *The National Law Review* https://natlawreview.com

First Health Insurance Portability and Accountability Act (HIPAA) Resolution Agreement of 2013 — and it certainly will not be the last

Article By:

Privacy & Security Practice Group at Mintz Levin

The HHS Office of Civil Rights (OCR) announced its first HIPAA Resolution Agreement of 2013 last week. According to the press release, Idaho State University (ISU) **must pay OCR $400,000 and comply with the terms of a two-year corrective action plan (CAP) to address violations of the HIPAA Security Rule**, which describes the technical, administrative, and physical safeguards against unauthorized access to electronic personal health information (ePHI).

ISU self-disclosed the exposure of the ePHI of approximately 17,500 patients at one of its health system's facilities in August 2011. The patients' ePHI had become compromised when ISU staff disabled firewall protections on a server for one of its 29 outpatient clinics. ISU officials did not discover the "hole" in the system's security for over ten months – a fact underlying OCR's determination that "**ISU's [privacy and security] risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities.**" The Resolution Agreement summarizes OCR's conclusions regarding ISU's deficient privacy and security processes after it completed an in-depth investigation pursuant to the self-disclosure:

- ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012;
- ISU did not adequately implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and
- ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.

As part of its two-year CAP, ISU must complete an initial compliance gap analysis regarding each Security Rule provision as well as Annual Reports summarizing any training, review measures and updates of its risk management plan and information system security measures. All in all, the ISU resolution is a prime example of OCR Director Leon Rodriguez's statement at last week's NIST-OCR conference that OCR is more likely to impose monetary penalties on "ongoing

violations” of sets of laws. (Our sister blog, Health Law and Policy Matters, provides more highlights of the conferencehere.)

Of note, ISU is a hybrid entity because it is an institution that has components other than its health clinics that perform activities that are not subject to HIPAA. Hybrid entities must be especially careful of properly identifying entities that must comply with HIPAA and appropriately structuring privacy and security policies that adequately meet the law’s standards. As Dianne Bourque, a Member of Mintz’sHealth Law Practice, points out, “An additional complexity for hybrid entity employees is remaining mindful of their privacy and security obligations for the covered component or components of the hybrid entity as distinct from the non-covered components. This is difficult when the hybrid operates as a single organization. Training is critical for entities like this.”

National Law Review, Volume III, Number 151