PUBLICATION

Is Your Firewall On? Are You Sure? Idaho State University Settles Privacy Rule Violations for $400,000 [Ober|Kaler]

2013: Issue 13 - Focus on HIPAA/Privacy

The HHS Office of Civil Rights (OCR) recently announced a $400,000 settlement with Idaho State University (ISU) following a lengthy investigation of the privacy and security practices at ISU outpatient clinics.

In addition to the monetary settlement ISU, was required to execute a two-year Corrective Action Plan (CAP) that requires ISU to identify itself as a "hybrid entity," make substantial changes to its risk analysis and management efforts, and submit annual reports.

ISU's troubles began in September 2011, when the university discovered that its server firewall had been disabled in August 2010 for maintenance and had never been restored. The university noted to local news media at the time that, although some "hackers" had accessed the server and used it to store pirated movie files, "there [was] no evidence that any of that medical information has been stolen or even accessed." The security lapse, however, exposed approximately 17,500 patient medical records, and was properly reported to OCR.

As has been the case with all breaches involving more than 500 individuals, OCR opened an investigation into ISU's HIPAA compliance. After determining that ISU failed to comply with requirements to properly assess the risk of a data breach and failed to properly monitor its systems, ISU and OCR reached the settlement described.

ISU's Violations

OCR's Resolution Agreement (RA) (which also attaches a copy of the CAP) provides some detail regarding the categories of noncompliance it identified as justifying the monetary settlement and CAP:

- 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."

The RA does not provide, of course, an explanation of the steps that ISU *had* taken, but seems to imply that ISU took *no steps* either to identify risks to its PHI or, perhaps more importantly, to actively monitor system activity to ensure that ePHI was not being improperly accessed. Similarly, the listing of violations does not cite to any specific regulation or standard to support OCR's determination that a violation had occurred (mostly because the standards at work, "reasonableness," "appropriateness," and "sufficiency," are not specifically defined in any regulation or guidance). That covered entities are required to both conduct an analysis of risks

posed to its PHI (including ePHI) and actively monitor systems where ePHI is stored, however, is a relatively well-settled principle.

ISU's CAP

A settlement with OCR generally requires not only a cash payment but also a commitment to a (generally, two year) Corrective Action Plan. (*For a detailed discussion of corrective action plans, see "Corrective Action Plans Can Mean Significant Compliance Monitoring Requirements."*) These plans are intended to ensure ongoing compliance much in the same fashion as Corporate Integrity Agreements are intended to ensure ongoing compliance following a settlement with the HHS OIG. The two agreements also obligate the provider to significant ongoing reporting and auditing responsibilities as well as potentially substantial costs related to a diversion of enterprise resources and the retention of (and satisfaction of) an outside auditor.

Given the scope of ISU's breach, its CAP might be seen as more lenient than one might expect. Notably, the CAP requires that ISU properly identify itself as a *hybrid entity* (an entity with some business units subject to HIPAA, and some not), submit annual reports and correct its security deficiencies, but it does not require the engagement of an outside monitor, the submission of monitor reports, or the imposition of any (announced or unannounced) site inspections. As we have noted in other articles, The imposition of the latter obligations are not unusual and can prove a costly burden to providers subject to a CAP. (*For a more detailed discussion of CAP requirements, see "$1.5 Million OCR HIPAA Settlement Provides Notice of Increased Enforcement Focus on Mobile Device Security and Encryption."*)

In the event that ISU fails to fulfill its responsibilities under the CAP, of course, it would remain subject not only to an additional investigation and any penalties resulting from the conduct that breached the CAP, but OCR would no longer be bound by the settlement's release.

Ober|Kaler's Comments

ISU's settlement, though unsurprising, is instructive in several ways:

- Security assessment and monitoring (and the documentation of those activities) are key to compliance with the Security Standards and a clear focus in recent OCR investigations. Covered entities and business associates should by now understand that active monitoring of systems containing ePHI is mandatory, but it is equally important to note that security assessment and monitoring that isn't well documented might as well not have happened. Every step in a provider's security process should be clearly documented by the entity's privacy or security officer (or a designee).
- When it comes to HHS OCR, no news is not necessarily good news. By statute, OCR must post a notice regarding all breaches affecting 500 or more individuals, and does so on its dedicated web page. It is not a short list. By policy, OCR has investigated (or will investigate) all of these large breaches. That a breach occurred two (or more) years ago is no guarantee that an investigation won't be undertaken or that penalties won't be forthcoming. Providers who experience a breach involving more than 500 individuals' PHI should expect an investigation and should be prepared to demonstrate the steps they have taken both before and since the breach to ensure and, where necessary, improve compliance.
- Finally, although not discussed in any of the publicly available materials surrounding the ISU settlement, it would be difficult to believe that post-breach responses (and perhaps some skillful negotiation) didn't play a large role in the settlement reached in this case. The ISU breach involved thousands of patients, went on for nearly a year, and was the direct result of a lack of basic system

monitoring – yet the OCR settlement is far less burdensome than others that involved fewer patients and far less surprising security lapses. Entities facing a breach should keep in mind that their post-breach actions, including notices sent, remediation efforts undertaken, and policy revisions implemented, will be reviewed just as closely as the mistakes that led to the breach. They should also keep in mind that a settlement is just that – and all settlements involve a good deal of negotiating.

** Joshua J. Freemire is a former member of Ober|Kaler's Health Law Group*