Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Idaho University to Pay $400,000 for HIPAA Violations: Lessons Learned and Resources to Avoid Penalties

Idaho University to Pay $400,000 for HIPAA Violations: Lessons Learned and Resources to Avoid Penalties

Insight — 5/22/2013

This week, Idaho State University agreed to pay $400,000 to settle HIPAA Security Rule violations that allegedly left the electronic health information of 17,500 patients accessible for at least 10 months. According to the Office of Civil Rights ("OCR"):

- ISU disabled firewall protections that would have otherwise protected the information on its servers.
- ISU's risk analyses and assessments of its affiliated clinics were inadequate.
- ISU failed to apply proper security measures and policies to address risks to the information.
- ISU did not have procedures for routine review of its system which could have detected the firewall breach much sooner.

All of these items were required by the Security Rule. The OCR's press release is located here.

This case offers several lessons for all providers and their business associates:

1. **The OCR is serious about Security Rule compliance.** Like most of the recent reported cases in which penalties were imposed, this case arose from the violation of the Security Rule. Many if not most providers have ignored or do not understand the specific, technical requirements of the Security Rule. This is the second time the OCR has imposed penalties on Idaho providers for Security Rule violations this year; even larger penalties have been imposed on entities in other states. The message is clear: providers must take Security Rule compliance seriously.
2. **Business associates beware.** In addition to providers, HIPAA now applies directly to business associates of providers. Business associates are those entities who create, maintain, receive or transmit protected health information on behalf of providers. Business associates must also comply with Security Rule requirements. Many business associates may not understand their HIPAA obligations.
3. **Perform and document a proper risk assessment.** The Security

Rule requires covered entities and business associates to perform, document, and periodically update a risk assessment of their information systems to ensure they have adequate policies and procedures to protect electronic health information. The OCR has published a guide for conducting appropriate risk assessments, which is available here.

4. **Implement the required Security Rule policies and procedures.** The Security Rule requires providers and business associates to implement specific administrative, physical and technical safeguards set forth in 45 CFR § 164.300 *et seq*. Implementing and documenting such safeguards are keys to avoiding HIPAA violations and, if violations occur, HIPAA penalties. The OCR has published a series of guides to help providers and business associates implement the Security Rule; the guides are found here.
5. **Respond immediately if you discover a potential breach.** Responding immediately may help avoid or mitigate security breaches. In addition, providers and business associates can avoid penalties altogether if (1) the violation did not result from willful neglect, and (2) they correct the problem within 30 days. It behooves providers and business associates to ensure they have the required safeguards in place and respond immediately to potential breaches, including making any necessary reports to individuals or HHS.

Holland & Hart HIPAA Resources. Holland & Hart has prepared resources to help clients and contacts comply with the HIPAA rules, including the following:

1. **A redlined copy of the Security, Privacy and Breach Notification Rules** which shows the changes made by the recent HIPAA Omnibus Rule. Click here to view.
2. **Checklists of required HIPAA polices.** Security checklist | Privacy checklist.
3. **Sample HIPAA Privacy Rule policies and forms.** For information concerning the policies and forms, contact kcstanger@hollandhart.com.
4. **Articles offering suggestions for complying with HIPAA**, including the new HIPAA Omnibus Rule requirements. The articles may be downloaded at http://www.hollandhart.com/healthcare/.
5. **HIPAA training webinar.** This hour-long webinar was originally presented as part of our *Health Law Basics* series. The recording may help entities satisfy HIPAA training requirements. The recording is available for download here.

We hope these resources will help our clients and friends comply with HIPAA and avoid the penalties.

For questions regarding this update, please contact
Kim C. Stanger
Holland & Hart, U.S. Bank Plaza, 101 S. Capitol Boulevard, Suite 1400,

Boise, ID 83702-7714
email: kcstanger@hollandhart.com, phone: 208-383-3913
