Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

HIPAA Penalties Come to Idaho: Secure Your Electronic Devices

HIPAA Penalties Come to Idaho: Secure Your Electronic Devices

Insight — 3/15/2013

Last week, an Idaho hospice agreed to pay $50,000 for HIPAA violations arising out of the theft of a laptop containing unencrypted health information of 441 patients. The case offers several lessons for all providers:

1. **Secure your electronic devices.** Like most of the recent penalties, this case sprang from loss of electronic data. The HIPAA security rule requires providers to take certain steps to secure electronic data. Proper encryption protects patient information and excuses providers from the obligation to self-report breaches. The recent epidemic of electronic breaches has caused the OCR to launch a special educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information* in December 2012. The program features online tools that may be accessed at http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security. Providers who use mobile devices should take heed.
2. **Breach notification does not protect you.** The hospice had to pay $50,000 even though it self-reported the breach. The fine is ominous given the Omnibus Rule's lower standard for breach notification, which will result in more reports and potentially more fines. Of course, the fines could have been much higher if the hospice was caught failing to report. According to HHS, the failure to report a breach evidences "willful neglect" triggering mandatory penalties of $10,000 to $50,000 per violation. A single breach can result in multiple violations, thereby multiplying the fines. On the whole, it's probably safer to report than to hide a breach.
3. **Make sure you have a documented risk assessment and implemented required policies.** While the theft of the laptop triggered the investigation, the penalties resulted from the hospice's failure to (1) conduct and document an appropriate risk assessment, (2) implement security policies or procedures, or (3) periodically update the assessment and policies, all of which are required by the HIPAA security rule. Again, according to HHS, the failure to implement required policies may evidence "willful neglect", resulting in mandatory penalties. In contrast, HHS has suggested that penalties may not be imposed despite a breach where the covered entity implemented required polices and safeguards; properly trained employees; and corrected any breach within 30 days. Implementing the required policies and safeguards is preventative medicine against HIPAA penalties.

4. **Even small cases can result in big fines.** The OCR touted this case as the first settlement involving less than 500 patients. As the OCR czar stated, "This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information"—including, and perhaps especially, unencrypted on mobile devices.

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
