KING & SPALDING

Health Headlines

March 19, 2012

HHS and BCBST Settle HIPAA Case for $1.5 Million

On March 13, 2012, HHS announced that Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay HHS $1.5 million to settle potential violations of the HIPAA privacy and security rules. In addition, BCBST agreed to a corrective action plan (CAP) to address alleged gaps in its HIPAA compliance program.

According to the HHS press release, the investigation followed a notice submitted by BCBST to HHS reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained audio and video recordings related to customer service telephone calls with PHI for over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. HHS concluded, based on its investigation, that BCBST failed to implement appropriate administrative safeguards to adequately protect the information at the leased facility because it did not perform the required security evaluation in response to operational changes. The information, however, was stored in a leased data closet secured by biometric and keycard scan security and in a building with additional security provided by the facility owner. Although BCBST received an alert that the server was unresponsive, the message did not alert BCBST that there may have been a theft and the server did not appear to adversely impact operations.

The corrective actions BCBST is required to implement under the CAP include:

- Development and implementation of policies and procedures that include a risk assessment and risk management plan, appropriate facility access controls and appropriate physical safeguards governing the storage of electronic media;
- Regular training for all BCBST employees who have access to ePHI;
- Reviews by a monitor, under the direction of BCBST's Chief Privacy Officer, to sample both the BCBST workforce members and BCBST electronic storage media and portable devices containing ePHI to confirm adherence to the required training, policies and procedures; and
- Unannounced site visits by the monitor to BCBST facilities housing portable devices.

If BCBST fails to fulfill the requirements of the CAP, HHS may impose civil monetary penalties as provided by the privacy and security regulations.

This enforcement action is the first resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, signaling that the government will pursue PHI data security breaches and impose severe fines and onerous corrective actions. Organizations should take a formal approach to data security compliance and demonstrate that they were diligent in their efforts to address physical security issues for PHI in addition to ensuring administrative and technical safeguards are in place. The starting point for any data security compliance is to do a thorough and well-documented risk assessment.

A copy of the settlement agreement and CAP is available by clicking **here**.

Reporter, *Lora L. Greene*, New York, +1 212 556 2174, lgreene@kslaw.com.

Health Headlines – Editor:

Dennis M. Barry
dbarry@kslaw.com
+1 202 626 2959