Health Information Compliance Alert

Take A Warning From The BCBST Case

This can happen to you.

HIPAA violations can burn a hole in your pocket unless you ensure data security religiously and are always vigilant to prevent breaches.

Leon Rodriguez, Director of the HHS Office for Civil Rights (OCR), announced on March 13, 2012 that "Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules," according to an HHS press release. This action followed BCBST's disclosure of the theft of 57 unencrypted computer hard drives from a leased facility in Tennessee.

It was BCBST's failure "to implement appropriate administrative safeguards to adequately protect information" which was thrown up the OCR's investigation. They should have been performing the required security evaluation in response to operational changes, according to the press release. In addition, the investigation showed a "failure to implement appropriate physical safeguards by not having adequate facility access controls," it added. Since both of these safeguards are required by the HIPAA Security Rule, Rodriguez pointed out that, "This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program."

According to the agreement BCBST will be required to review, revise, and maintain its Privacy and Security policies and procedures, in addition to the $1,500,000 settlement, the press release said. Further it will have to conduct "regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA." To ensure BCBST compliance with the corrective action plan, it will need to perform monitor reviews as a regular process.