

## HHS Settles HIPAA Case for \$1.5 Million

---

March 22, 2012

---

On March 13, 2012, HHS announced a settlement with Blue Cross Blue Shield of Tennessee (BCBST) regarding potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. The investigation by HHS arose after a November 2009 breach report notice submitted by BCBST to HHS reported that 57 unencrypted computer hard drives containing protected health information (PHI) of more than 1 million individuals were stolen from a leased facility in Tennessee. As a result of its investigation, HHS discovered that BCBST failed to implement appropriate administrative and physical safeguards to adequately protect PHI. In addition to the \$1.5 million penalty, the settlement agreement requires BCBST to review, revise and maintain its Privacy and Security Policies and Procedures and to conduct regular trainings for all BCBST employees with responsibilities under HIPAA. According to HHS, this enforcement action is the first resulting from the breach report required by the Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification Rule. The settlement also serves as reminder to health plan sponsors to conduct regular reviews of their HIPAA Policies and Procedures because the penalties for noncompliance can be substantial. The press release from HHS is available [here](#).