eALERT

INCompliance

March 16, 2012

First Enforcement Action Under HITECH Breach Rules Results in $1.5M Settlement by Blue Cross Blue Shield of Tennessee

On March 13, 2012, the Department of Health and Human Services ("HHS") announced that Blue Cross Blue Shield of Tennessee ("BCBST") agreed to pay $1,500,000 to settle potential violations of the HIPAA Privacy and Security Rules. This represents the first enforcement action resulting from the HITECH Act breach notification rules.

BCBST notified HHS under the breach reporting requirements the theft of 57 unencrypted computer hard drives from a facility that BCBST leased. The hard drives contained protected health information, including names, social security numbers, diagnosis codes, and dates of birth, of over one million individuals. BCBST was in the process of moving operations from the leased facility when the breach occurred. BCBST had surrendered most of the leased property except for a network data closet that contained the hard drives. BCBST had turned security of the network closet over to the property owner after BCBST staff had vacated the building.

The HHS press release states that the Office for Civil Rights ("OCR") investigation indicated that "BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes." Further, OCR announced that the investigation "showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule."

In addition to the $1,500,000 settlement, BCBST entered into a corrective action plan ("CAP") with HHS. Under the CAP, no liability was admitted and BCBST expressly denied liability as a result of the theft. As part of the CAP, among other things BCBST agreed to: (1) conduct a risk assessment of potential risks and vulnerabilities to ePHI when it is created, received, maintained, used, or transmitted on or off-site; (2) maintain facility access controls and a facility security plan to limit access to electronic information systems and facilities where they are housed and to safeguard equipment containing ePHI from unauthorized physical access, tampering, and/or theft; (3) conduct monitoring including random audits of electronic media storage and unannounced site visits to BCBST locations housing portable devices; and (4) submit two biannual reports to HHS certifying compliance with the requirements of the CAP.