MINTZ

The cost of HIPAA non-compliance – $17 million - UPDATE

March 19, 2012| Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Written by Kevin McGinty

If it wasn't clear before, a recent settlement of HIPAA claims brought by the Department of Health and Human Services against BlueCross BlueShield of Tennessee ("BCBST") underscores the high regulatory cost of non-compliance with privacy requirements. HHS announced on March 13, 2012 that BCBST has agreed to pay $1.5 million to settle claims that BCBST violated HIPAA in connection with the theft in 2009 of 57 unencrypted hard drives containing protected health information of over 1 million individuals. The payment to HHS, however, is the tip of the iceberg. **According to the Nashville Business Journal**, BCBST reported that it has spent nearly $17 million in investigation, notification and protection efforts. Thus, even though privacy class actions typically falter for inability to prove recoverable damages, the BCBST case demonstrates that data breaches can still result in substantial administrative fines and remediation costs.

The clear takeaway: Businesses should be mindful of the potential cost of non-compliance when evaluating the sufficiency of their privacy-related policies, procedures and infrastructure.

UPDATE: And, further analysis from our colleagues over at the Mintz Health Law Policy blog -- **here**

Authors

Cynthia J. Larose, Member / Chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.