

Tennessee Health Plan Pays \$1.5 Million for Data Security Problems

APRIL 30, 2012

The Tennessee BlueCross BlueShield health insurance plan suffered a data breach in 2009, and as required by the HITECH Breach Notice law, submitted a report about the breach to the Department of Health and Human Services (HHS). Commentators have noted that the breach suffered by the Tennessee Blue Plan was routine, namely that several of its hard drives were stolen. According to an HHS investigation though, the plan had provided insufficient protection for the health information located on those stolen drives. As a result, the parties settled with not only a payment of \$1.5 million, but also a promise by the plan that it would put in place specific policies and procedures to better protect health information. Those included conducting a risk assessment, creating a risk management plan, putting in place facility access controls and a facility security plan, implementing physical safeguards, and conducting employee training. The settlement also required the plan to report to HHS that the policies have been put in place, and random compliance monitoring (including unannounced site visits).

TIP: This settlement is not only a reminder for those subject to HIPAA that they must have strong data protection policies and programs in place, but also can serve as helpful guidance for other industries about what types of procedures to put in place to protect sensitive data.

1 Min Read

Related Topics

Health Care Privacy

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.