Health Insurer's Costly Privacy Breach Provides Guidance For Managing HIPAA Risks Associated With Electronically-Stored PHI

03.29.2012
03.29.2012

In the first enforcement action resulting from a reported privacy breach under the HITECH Act, Blue Cross and Blue Shield of Tennessee ("BCBST") recently entered a $1.5 million settlement with the U.S. Department of Health & Human Services following the theft of 57 hard drives from a former BCBST call center. When the theft occurred in October 2009, BCBST had already ceased operations at the facility, but was continuing to maintain the hard drives in secure data storage located there pending remediation scheduled to take place the following month. After the theft, BCBST promptly reported the breach to HHS and later determined that the stolen hard drives contained a considerable amount of PHI of its members, primarily in the form of audio recordings of customer service phone calls.

In the immediate aftermath of the theft of the hard drives (which contained unencrypted data), BCBST quickly launched a company-wide effort to inventory all of its electronically-stored PHI ("ePHI") and eventually encrypted 885 terabytes of ePHI at a cost of $6 million. In total, BCBST spent $17 million investigating the breach, notifying the members affected by the theft, and implementing security measures to protect ePHI in the future. Nevertheless, HHS required the company to pay $1.5 million and implement a series of corrective measures to settle the HIPAA violation.

While the amount that BCBST spent to remediate and resolve this matter underscores the importance of proper information governance of ePHI, the voluntary remedial efforts that BCBST undertook following the theft, and the corrective measures to which it agreed in the HHS settlement, provide a clear framework for managing and mitigating the privacy risks associated with ePHI, including:

1. Conduct a company-wide inventory of all data repositories, including mobile devices and flash-drives, where ePHI resides;

2. Encrypt all at-rest ePHI to prevent access in the event of a breach or theft;

3. Adopt internal policies and procedures governing the handling and storage of ePHI

that are consistent with the requirements of the HIPAA Privacy and Security Rules;

4. Train all employees with access to ePHI on the policies and procedures, and audit compliance on a regular basis;

5. Ensure that only properly trained employees are involved in the handling, storage, or transportation of ePHI;

6. Conduct a comprehensive risk assessment regarding the confidentiality, integrity and availability of ePHI;

7. Develop a risk management plan to implement security measures sufficient to reduce identified risks "to a reasonable and appropriate level;" and

8. Implement facility-level security measures and safeguards to limit and control physical access to information systems in which ePHI is stored.

Although application of this framework will not immunize a company in the event of a HIPAA breach, it should help to reduce the likelihood of such a breach in the first instance, contain the scope of any breach that does occur, and prove useful in any discussions with HHS about resolving a breach. Given the ubiquity of electronic medical records and ePHI, the financial impact of the hard drive theft on BCBST highlights the critical importance for every health insurer, hospital, medical practice, long-term care facility, or other company storing ePHI to adopt, implement, and enforce effective information governance policies and practices to ensure the privacy, security, and integrity of all such data.

For more information about this topic, please contact the author or any member of the Williams Mullen eDiscovery and Information Governance Team.

Related People

Related Services

- eDiscovery and Information Governance
- Senior Housing Transactions

- Health Care