Covered Entity Agrees to Pay $1.5 Million After Self-Reporting HIPAA Breach

Legal Alert
March 29, 2012

Garvey Schubert Legal Update, March 2012.

View alert (PDF).

Background

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires covered entities to report certain breaches of protected health information (PHI). On November 3, 2009, Blue Cross Blue Shield of Tennessee (BCBST) submitted a HITECH Breach Report to the Office for Civil Rights (OCR) stating that 57 hard drives containing PHI for over one million individuals had been stolen on October 2, 2009.

In March of 2012, OCR announced that BCBST agreed to pay $1.5 million to settle alleged violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This $1.5 million payment represents the first enforcement action instigated by a covered entity self-reporting a HIPAA breach as required by the HITECH Act. In addition to paying $1.5 million, BCBST also agreed to implement a Corrective Action Plan.

Facts

BCBST housed its encoded computer hard drives in a network data closet in leased space maintained by the property management company. At the time of the data loss, BCBST was in the process of moving locations so that the server and hard drives were in a building separate from their new location. However, the building housing the network data did have building security and the network data closet was secured by biometric and keycard scan security with a magnetic lock and an additional door with keyed lock.

Sometime on Friday, October 2, 2009, BCBST received an alert that the server was “unresponsive.” Rather than respond on Friday, BCBST waited until Monday, October 5, 2009, to respond or investigate.

When BCBST investigated they found that fifty-seven hard drives containing unencrypted information for more than one million individuals had been stolen. The unencrypted information stolen included PHI of health plan members such as names, member ID numbers, diagnosis codes, dates of birth and social security numbers.

BCBST claims that after the breach it spent approximately $17 million for its investigation, breach notifications, and other protection efforts. Further, BCBST reports that it is voluntarily moving toward encrypting all of its at-rest data. BCBST also reports that there have not been any indications that any of the stolen PHI or other personal data has been misused. March 2012 2 OCR states that it found evidence that BCBST failed to implement appropriate administrative safeguards by failing to perform proper security evaluations and failure to implement appropriate physical safeguards because the building where the data was stored failed to have adequate access controls.

Lesson Learned

At first blush it is difficult to square the fact that the network data closet in question was secured by biometric and keycard scan security with a magnetic lock and an additional door with keyed lock with OCR's claim that BCBST failed to implement adequate physical safeguards because the building where the data was stored failed to have adequate access controls.

However, the Resolution Agreement and Corrective Action Plan (CAP) focus on a couple of key issues that may provide clues why OCR imposed a $1.5 million penalty on a covered entity that appears to have been in substantial compliance with HIPAA/HITECH. The negotiated settlement and CAP emphasize having current HIPAA Privacy and Security Policies and Procedures in place and ensuring that the workforce has had proper education and training on those policies and procedures.

Given this emphasis it seems reasonable to conclude that at least part of what drove OCR to impose the penalty was a concern that workforce members were not sufficiently trained to react immediately to information that the company's server was "unresponsive." Workforce members became aware that the company server, located in a separate building, was "unresponsive" on a Friday. Rather than investigate immediately why the server containing over one million records with PHI was "unresponsive," no one investigated until the following Monday.

At least one of the lessons to be learned here is that if you receive information that is out of the ordinary such as your server containing over one million records is suddenly "unresponsive," do not wait two or three days to investigate.

Conclusion

Policies and procedures implementing HIPAA safeguards must be established in writing but also have to be actively implemented by the workforce. It is therefore crucial that all employees and workforce members receive adequate training on those policies and procedures so that they are effectively implemented.