OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe | Health Law Group | Health Law Alert Archive

2012 Issue 4

www.ober.com

HITECH Breach Enforcement Announced: BCBS Settles with OCR for $1.5 Million

By: Sarah E. Swank and Joshua J. Freemire

Blue Cross and Blue Shield of Tennessee (BCBST) will pay $1.5 million and enter into a Corrective Action Plan with the Department of Health and Human Services Office for Civil Rights (OCR) to settle OCR's investigation into BCBST's violations of the HIPAA Security Rule. Sarah Swank and Joshua Freemire review the genesis of the settlement and discuss the lessons other covered entities can learn from it.

Increased enforcement is a key message from the Department of Health and Human Services Office for Civil Rights (OCR). Since the start of 2012, OCR has publicized settlements with three entities: two of which concerned civil rights violations under section 504 of the Rehabilitation Act and the most recent of which concerned violations of the HIPAA Security Rule. On March 13, 2012, OCR issued a press release detailing its settlement with Blue Cross and Blue Shield of Tennessee (BCBST), under which BCBST agreed to pay $1.5 million and enter into a 450-day Corrective Action Plan (CAP) to address its HIPAA compliance issues. BCBST settled following an investigation triggered by the report of a "breach" — 57 unencrypted hard drives, including patient records for over a million patients, were stolen from a leased facility in Tennessee.

The Breach

BCBST's troubles began when it was discovered that the 57 hard drives apparently had been stolen. The hard drives were located in a network data closet on a leased premise that BCBST vacated. The drives were part of a system that recorded and stored audio and video recordings of customer service calls, including protected health information (PHI) such as member names, social security numbers, diagnosis codes, dates of birth and health plan identification numbers. This information was not

encrypted. After BCBST reported the breach to OCR as required, OCR initiated an investigation that concluded the theft may have occurred as a result of BCBST's failure to appropriately implement required Security Rule procedures.

OCR's press release explains that BCBST was not penalized as a result of the breach itself. Rather, BCBST faced penalties because it "failed to implement appropriate administrative safeguards to adequately protect information remaining at [a] leased facility by not performing the required security evaluation in response to operational changes" and failed "to implement appropriate physical safeguards by not having adequate facility access controls." According to OCR, the HIPAA Security Rule requires both steps to safeguard information on the hard drives.

The Settlement

In addition to the monetary settlement, BCBS was required to enter into a CAP [PDF]. Much like corporate integrity agreements (CIAs), OCR's CAPs require that covered entities make certain changes to existing HIPAA policies and procedures, submit regular reports, report any compliance failures ("reportable events") and agree to periodic monitoring by internal or external monitors. Importantly, a violation of the CAP reopens OCR's investigation into not only the event that gave rise to the violation of the CAP, but also the initial event or events that resulted in the CAP. A violation of the CAP could mean that BCBST pays the $1.5 million under the settlement plus faces additional civil money penalties pursuant to 45 CFR part 160 for any violations of the CAP.

BCBST's CAP is arguably less burdensome than some other CAPs from OCR. Under the agreement, BCBST must modify many of its HIPAA policies and procedures and submit them for OCR review. It also must conduct additional employee training within certain timelines, and report any breaches of the new policies directly to OCR. BCBST's CAP, like many, requires monitoring and regular reporting to OCR, but in BCBST's case, the monitoring will be conducted by the company Compliance Officer, rather than an external entity. BCBST's Compliance Officer is required to conduct two "Monitor Reviews" (which include unannounced site visits, interviews, and inspection of portable devices) and submit to OCR two

semi-annual reports detailing the results and attesting to compliance with CAP provisions. The term of the CAP is also fairly short – just 450 days.

HITECH Reporting

The Interim Final Breach Notification Rule requires covered entities to inform both HHS and affected individuals when protected health information has been improperly used or accessed (a "breach"). Covered entities must also report breaches involving 500 individuals or more to the media. OCR automatically initiates an investigation into any breach that affects more than 500 individuals. The results of its investigations are available on a dedicated website. As of August 12, 2011, OCR received 300 reports involving over 500 individuals and over 34,000 reports involving under 500 individuals.

Enforcement Increases But Some Room to Negotiate

There can be little doubt that OCR intends to more aggressively pursue HIPAA/HITECH enforcement. OCR Director Leon Rodriguez stated in the news release that, "This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program." Covered entities and business associates should note that BCBST's troubles arose from a lack of encryption. Regardless of the theft of the hard drives, if the missing drives had been encrypted, there would have been no "breach" to report and no further investigation by OCR. Encryption, of course, should never take the place of sound, reasonable, and compliant security policies consistent with the HIPAA Security Rule. Finally, covered entities and business associates who report a breach should note that CAPs, depending on the situation, may be negotiable. By focusing on key terms in the CAP, such as who will conduct monitoring reviews, the frequency of those reviews, and the term of the CAP, those who must enter into CAPs can hope to keep the cost of compliance at a minimum. (For more on CAPs generally, read our analysis of existing CAPs.)