MANAGED CARE OUTLOOK

The Insider's Business Briefing on Managed Healthcare

ASPEN PUBLISHERS

Volume 25, Number 8 • April 15, 2012

HHS Imposes First Civil Penalty and Resolution Agreement Resulting from HITECH Breach Notification Rule

M. Leeann Habte

R. Michael Scarano, Jr.

Peter F. McLaughlin

On March 13, 2012, the Office for Civil Rights (OCR) carried out its first enforcement action resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Blue Cross Blue Shield of Tennessee (BCBST) entered into a resolution agreement with OCR in which it agreed to pay $1.5 million and enter into a corrective action plan (CAP) to address its Health Insurance Portability and Accountability Act (HIPAA) compliance program. In announcing the agreement with BCBST, OCR Director Leon Rodriguez stated that the enforcement action sends an important message that OCR expects carefully designed, delivered, and monitored HIPAA compliance programs.

Issued in August 2009, the Breach Notification Rule requires covered entities under HIPAA to report certain breaches to OCR. Although there have been a number of settlements arising from alleged HIPAA violations based on complaints to OCR, this is the first sign of OCR's approach to enforcement based on self-reports of breaches by covered entities. According to OCR, the HIPAA breach notification requirements are an important tool in its enforcement strategy, which also includes HIPAA compliance audits and training state attorneys general and their staffs to use their new authority under the HITECH Act to enforce the HIPAA privacy and security rules in civil actions. (See Foley's prior Alert, *HHS Initiates Pilot Audit Program for HIPAA Compliance*, and Foley's blog post, *Office of Civil Rights Establishes Corrective Action Plans and Resolution Payments as Key Enforcement Tools*, both available at www.foley.com.)

OCR Investigation Shows BCBST Failed to Comply with HIPAA Safeguards

BCBST had self-reported the potential breach of privacy arising from the theft of 57 hard drives from a network data closet in a leased facility that had been vacated by all BCBST staff. The hard drives, which contained data that were encoded but unencrypted, stored more than 300,000 video recordings and one million audio recordings, which stored the protected health information (PHI) of about one million individuals. OCR's investigation indicated that BCBST had not implemented appropriate administrative physical safeguards to adequately protect the information in that 1) it did not perform the required security evaluation in response to operational changes, and 2) it failed to implement appropriate physical safeguards by not having adequate facility access controls. In response to the theft, BCBST undertook a $6 million effort to encrypt all at-rest data throughout its enterprise, which was reported to be successfully completed in July 2011.

In addition to paying the $1.5 million settlement, BCBST entered into a CAP with HHS, which requires BCBST to create adequate policies and procedures addressing risk assessment, risk management, and physical security, and to increase training of employees and monitoring of their compliance with BCBST HIPAA policies.

Practical Advice for Covered Entities

In light of OCR's recent enforcement actions, covered entities should consider the following:

- Covered entities should give increased attention to the physical security plans for their facilities. Adequate physical safeguards are essential to preventing breaches of PHI.
- Covered entities should ensure their compliance program policies and procedures are up to date and incorporate new HIPAA developments and changes. The HIPAA regulations have undergone significant change as a result of amendments made by the HITECH Act, including the Breach Notification Rule. A proposed rule implementing certain other parts of the HITECH Act was published on July 14, 2010 (75 FR 40868), but the final rule has not yet been issued. It is expected to be released soon. Covered entities will need to review the final rule and comply with it once it is effective.
- Covered entities should verify that their actual practices regarding HIPAA privacy and security conform to the requirements in their written policies and procedures. In addition, both their policies and procedures and their actual practices must keep pace with changes in their operations.
- Staff should be periodically trained and educated on relevant privacy and security requirements under both HIPAA and any applicable state privacy laws.

Conclusions and Implications

The number of OCR investigations that have resulted in corrective action has more than doubled since 2003. OCR's resolution agreement with BCBST may foreshadow more vigorous enforcement of the HIPAA privacy and security rules. Covered entities should examine their current HIPAA policies and practices to verify that the entity's operations are current and consistent with the recent legal changes. For businesses subject to these rules, collaboration with health care counsel knowledgeable about HIPAA is an important step in protecting against enforcement exposure and helping ensure compliance. ■

M. Leeann Habte is an associate with Foley & Lardner LLP and can be reached at lhabte@foley.com. **R. Michael Scarano, Jr.** is a partner with Foley & Lardner LLP and is vice chair of the firm's Health Care Industry Team. He can be reached at mscarano@foley.com. **Peter F. McLaughlin** is senior counsel with Foley & Lardner LLP and a member of the firm's Privacy, Security & Information Management and Information Technology & Outsourcing Practices. He can be reached at pmclaughlin@foley.com. All three authors are members of the firm's Health Care Industry Team.

The authors wish to acknowledge the significant contribution of Law Graduate Danna Carmi to this article.