HINSHAW

Alerts

HIPAA Privacy and Security HITECH Act Enforcement Actions Begin

April 11, 2012
Health Law Alert

The Health Insurance Portability and Accountability Act Health Information Technology for Economic and Clinical Health Act (HIPAA HITECH) data-breach final rule requires entities to report unsecured data breaches. As of this date, the U.S. Department of Health and Human Services (HHS) has received 410 reports of unsecured data breaches affecting 500 or more individuals. The two recent enforcement actions discussed below signal an era of heightened HIPAA enforcement. In light of these enforcement activities, health care providers and their counsel should immediately: review their HIPAA privacy and security compliance programs; continuously audit and monitor their privacy and security practices; regularly train employees on handling protected health information; and document all aspects of their HIPAA privacy and security compliance program implementation.

Health Insurer Agrees to Pay $1.5 Million Settlement for Enforcement Action Resulting From a HIPAA HITECH Act Breach Report

On March 13, 2012, the HHS Office of Civil Rights (OCR) announced the first enforcement action resulting from a breach self-report required by HITECH's breach notification rule. Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay OCR $1.5 million and to take certain other actions specified in a corrective action plan to avoid civil monetary penalties for charges of HIPAA violations. According to published reports, in addition to the OCR fine, BCBST has spent more than $17 million in costs related to investigation, notification and protection efforts. In addition, BCBST has estimated that more than 300 of its employees have worked on duties related to the breach. The BCBST breach demonstrates the significant monetary exposure that can result from unintentional noncompliance with HIPAA privacy and security requirements.

HIPAA Security Breaches. On October 5, 2009, BCBST employees discovered a theft of computer equipment from a network data closet located at an office location in Chattanooga, Tennessee. BCBST's internal investigation found that the theft occurred on or about October 2, 2009. The stolen items included 57 hard drives containing encoded electronic data. The hard drives that were stolen contained data that included the protected health information (PHI) of health plan members, such as member names, member identification numbers, diagnosis codes, dates of birth, and Social Security numbers. BCBST's internal investigation confirmed that the PHI of 1,023,209 individuals was stored on the hard drives.

Attorneys

Michael A. Dowell

The Breach Notification Rule. The HIPAA/HITECH breach notification rule requires covered entities to report a breach (e. g., an impermissible use or disclosure of protected health information that compromises the security or privacy of the protected health information) to the affected individual(s), HHS and, at times, the media. The definition of breach is subject to several qualifications and exceptions that require a case-by-case analysis to determine whether or not a breach has occurred. Once it is determined that a breach has occurred, affected individuals must be notified within 60 days of the discovery of the breach. If the breach affects more than 500 individuals, HHS and the media must be notified. BCBST notified HHS under the breach reporting requirements regarding the theft of the stolen hard drives containing protected health information for over one million individuals.

The Settlement. OCR conducted an investigation based on the BCBST breach report. According to OCR's investigation, BCBST failed to implement appropriate administrative and physical safeguards as required by the HIPAA security rule. More specifically, BCBST failed to perform the required security evaluation in response to operational changes and did not have adequate facility access controls. In addition to the $1.5 million settlement, the Resolution Agreementbetween BCBST and OCR requires BCBST to comply with a corrective action plan. The corrective action plan obligates BCBST to: (1) develop and implement policies and procedures that include a risk assessment and risk management plan, appropriate facility access controls and appropriate physical safeguards governing the storage of electronic media; (2) distribute those policies and procedures to all members of its workforce who have access to electronic PHI; (3) provide regular training for all BCBST employees who have access to electronic PHI (ePHI); (4) conduct random monitor reviews, including site visits and interviews of workforce members, to ensure that its workforce members are complying with BCBST's policies and procedures; (5) have compliance reviews by a monitor, under the direction of BCBST's Chief Privacy Officer, to sample both the BCBST workforce members and BCBST electronic storage media and portable devices containing ePHI to confirm adherence to the required training, policies and procedures; (6) maintain facility access controls and a facility security plan to limit access to electronic information systems and facilities where they are housed and to safeguard equipment containing ePHI from unauthorized physical access, tampering, and/or theft; and (7) have unannounced site visits by the monitor to BCBST facilities housing portable devices. Lastly, the corrective action plan requires BCBST to submit two biannual reports to OCR that document the training efforts and monitor reviews, and to retain all records pertaining to compliance with the plan for three years.

Implications of the Enforcement Action. "The 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," said OCR Director Leon Rodriguez. "The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients' right to private and secure health information."

Covered entities are urged to heed OCR's warning by strengthening their HIPAA compliance and adopting other suitable safeguards to minimize HIPAA exposures. The BCBST settlement is significant as the first reported enforcement action directly resulting from the filing by a covered entity of a breach report required by the HITECH Act breach notification rule, and the first reported resolution agreement reached with a covered entity that is a health plan. The enforcement action demonstrates the rule's significance as an OCR-HIPAA-enforcement tool, the heightened exposure to an OCR opening a HIPAA civil monetary penalty (CMP) investigation following a breach report, as well as the willingness of OCR to sanction health plans and other covered entities that breach HIPAA's privacy or security rules.

The BCBST settlement reemphasizes the importance for covered entities and their business associates to continually evaluate, monitor, audit and appropriately manage their HIPAA responsibilities. Covered entities should ensure that their privacy and security compliance and training programs are documented in accord with HIPAA specifications. Covered entities should also consider encryption of all of its at-rest data, so that the data will not be subject to the breach notification rule, and the purchase of data-security-breach insurance to pay the costs of responding to data breaches.

First HIPAA Enforcement Action against a Business Associate

In the first HIPAA enforcement action against a business associate, Minnesota Attorney General Lori Swanson filed a civil lawsuit (*Minnesota v. Accretive Health, Inc.* (No. 12-145 (D. Minn. Jan. 19, 2012), ECF No. 1) in federal court against HIPAA business associate Accretive Health, Inc. (Accretive) for alleged violations of HIPAA, Minnesota medical privacy law, consumer debt collection practices laws, and for violating privacy and security terms of business associate agreements with two Minnesota hospitals. The lawsuit was filed pursuant to powers granted to state attorneys general

(AGs) under HITECH provisions that expanded the enforcement powers and civil penalties applicable to HIPAA violations.

Business Associate Functions and Loss of Protected Health Information. Accretive contracted to act as a business associate to two Minnesota hospitals by providing debt collection, revenue-cycle management, data-mining, skip-tracing, per-patient risk-score calculation and patient-behavioral-modeling services. In this capacity, Accretive gathered PHI and quantified 22 various medical conditions, including bipolar disorder, schizophrenia, depression, high blood pressure, asthma, low back pain, HIV status and heart disease, to model patient behavior in an attempt to identify areas for cost reduction. The lawsuit followed the theft of an unencrypted, password-protected laptop from an Accretive employee's car that contained the individually identifiable health information of approximately 23,531 hospital patients. The information included patients' names, addresses, phone numbers, Social Security numbers and certain clinical information, including information related to chronic conditions such as mental health and HIV/AIDS conditions.

The Privacy and Security Breach Complaint Allegations. The AG complaint alleged eight security violations of HIPAA, including Accretive's failure to implement appropriate safeguards to protect patient data and adequately train members of its workforce. It also alleged that Accretive's failure to affirmatively disclose to patients the amount of health information they were collecting violated the Minnesota Prevention of Consumer Fraud Act and Uniform Deceptive Trade Practices Act. The complaint further alleged that Accretive violated HIPAA by failing to comply with the standards, requirements and implementation specifications as set forth in HIPAA, including the following:

- Failure to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. §164.308(a)(1).
- Failure to implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and to prevent those workforce members who do not have authorized access from obtaining access to electronic protected health information in violation of 45 C.F.R. §164.308(a)(3-4).
- Failure to effectively train all members of its workforce, including agents and independent contractors involved in the data breach, on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.308(a)(5).
- Failure to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that were known to them in violation of 45 C.F.R. §164.308(a)(6).
- Failure to implement policies and procedures to limit physical access to its electronic information systems in violation of 45 C.F.R. §164.310(a)(1).
- Failure to implement policies governing the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility in violation of 45 C.F.R. §164.310(d)(1).
- Failure to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1).
- Failure to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of Part 164, Subpart C in violation of 45 C.F.R. §164.316.

Potential Fines, Penalties and Judicial Relief. Attorney General Swanson is seeking a permanent injunction against Accretive as well as statutory damages for violations of HIPAA and various other Minnesota state laws, and reasonable attorneys fees. The penalties may range from $100 - $50,000 per violation.

Implications of the Enforcement Action. This case demonstrates the increasing interest on the part of state AGs to enforce HIPAA, as Connecticut, Indiana and Vermont AGs also filed enforcement actions last year following health information breaches. Business associates should confirm, through audits and monitoring, that they are currently complying with HIPAA privacy and security requirements of HITECH.

For more information, please contact Michael A. Dowell, or your regular Hinshaw attorney.

This alert has been prepared by Hinshaw & Culbertson LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship.