Bloomberg BNA

Health IT Law & Industry Report™

VOL. 4, NO. 0 AUGUST 20, 2012

Minnesota AG Reaches First Settlement With Business Associate Under HITECH Act



BY DANNA CARMI, LEEANN HABTE, AND MICHAEL SCARANO

On July 30, 2012, Minnesota Attorney General Lori Swanson announced a settlement agreement with Accretive Health (''Accretive'') resolving a lawsuit filed against Accretive in January 2012. The settlement requires Accretive to stop doing business in Minnesota for two years and to pay about $2.5 million to the State of Minnesota, a portion of which will be used to compensate patients.

Danna Carmi is an associate with Foley & Lardner LLP, Los Angeles, and a member of the firm's Health Care Industry Team. She may be reached at dcarmi@foley.com. Leeann Habte is an associate with Foley & Lardner LLP, Los Angeles, and a member of the Health Care Industry Team and Privacy, Security & Information Management Practice. She may be reached at lhabte@foley.com. Michael Scarano is a partner with Foley & Lardner LLP, San Diego, and vice chair of the Health Care Industry Team. He may be reached at mscarano@foley.com.

The lawsuit alleged that Accretive violated several provisions of the Health Insurance Portability and Accountability Act of 1996 (''HIPAA''), as modified by the Health Information Technology for Economic and Clinical Health (''HITECH'') Act, as well as other state and federal laws.

The case is significant because it represents the first enforcement action against a business associate under the new provisions of the HITECH Act that make business associates directly and statutorily liable (rather than only contractually liable) for violations of HIPAA and, in particular, for breaches of Protected Health Information (''PHI''). (Although the AG alleged in the alternative that Accretive was a covered entity, it relied primarily on its status as a business associate.) The case also illustrates aggressive use of the enforcement authority granted by HITECH to state attorneys general.

 ISSN 2151-2876

Complaint Initially Focused on Violation of Federal Privacy Law

Accretive contracts with hospitals to manage their revenue cycles. In the course of fulfilling its contractual obligations, Accretive gains access to the PHI of hospital patients and, as a business associate of covered entities, must comply with the HIPAA security provisions and certain privacy provisions.

In July 2011, an unencrypted laptop was stolen from the rental car of an Accretive employee. Swanson alleged that the laptop contained sensitive data, including Social Security numbers in some cases, on over 23,000 patients. (The federal Department of Health and Human Services report lists the breach tally as 16,800 patients.)

She further alleged that Accretive violated federal security laws by failing to encrypt PHI on laptops, allowing employees to take the laptops containing PHI out of hospital facilities, failing to effectively train its workforce members to maintain the security of PHI, and failing to identify and respond to the theft of PHI, among other violations.

In June 2012, Swanson amended her complaint to add that Accretive failed to execute a business associate agreement before receiving PHI, failed to implement security safeguards that could have protected the theft of the PHI, and gave its employees information that exceeds the minimum necessary information needed to perform their jobs.

The incident triggered a broader investigation of Accretive's business practices by the Attorney General. The case gained national prominence when Swanson issued a report, adding a myriad of allegations that Accretive violated several Minnesota state laws by, for example, engaging in deceptive, abusive, and aggressive collection practices. She accused the company of using high-pressure tactics to get patients at hospitals to pay before treatment was given, and said the company misused private patient information and created an atmosphere in which employees were coached to aggressively collect debt.

These actions prompted at least two federal investigations, including a Senate hearing in May of 2012.

Attorney General's Settlement With Accretive Health

To resolve the dispute, Accretive agreed to pay the settlement amount and to cease all operations in Minnesota within 90 days after the Settlement Agreement, or by Nov. 1, 2012. The company will then be subject to an outright ban on operating in Minnesota for two years, after which, for the next four years, it can only re-enter the State if the Attorney General provides specific permission and Accretive enters into a Consent Decree regarding its business practices in the State.

The settlement illustrates that business associates, as well as covered entities, can face serious consequences for perceived violations of privacy laws.

In addition, Accretive agreed to destroy or return all PHI and personal financial information that it collected on behalf of Minnesota clients within 60 days of shutting down its operations in the State and to pay for a nationally recognized independent consultant agreed upon by the Attorney General (whose agreement shall not be unreasonably withheld) to confirm, to reasonable industry standards, that the PHI and Personal Financial Information were removed.

Although Accretive did not admit any liability or wrongdoing, the cumulative costs to Accretive Health went far beyond the payment amount in the Settlement Agreement. In addition to the $2.5 million settlement, Accretive reported $12.7 million in lost operating margin and personnel costs associated with the settlement, which it projects will result in the loss of more than 100 jobs in Minnesota, along with $1.9 million in legal defense and crisis management costs, according to reports by Business Wire.

State Attorneys General Used New Enforcement Authority, Business Associate Requirements Under HITECH

Pursuant to the HITECH Act, business associates, like Accretive, are responsible for employing appropriate administrative, physical, and technical safeguards established under the HIPAA Security rule and promptly reporting breaches of PHI to covered entities, to allow for the notification of individuals and the mitigation of any risk to individuals resulting from such breaches. Business associates are also responsible for complying with the minimum necessary standards set forth in the HITECH Act.

HITECH also expanded the enforcement of HIPAA by granting authority to state attorneys general to bring civil actions and obtain damages on behalf of state residents for violations of HIPAA. In 2011, the Office for Civil Rights provided five regional training sessions to assist state attorneys general and their staff to implement this new authority.

Attorneys general in Connecticut and Vermont have previously taken enforcement actions against covered entities, both of which resulted in monetary settlements, but the Accretive case is the first such attorney general settlement involving a business associate.

Practical Advice for Covered Entities, Business Associates

The settlement illustrates that business associates, as well as covered entities, can face serious consequences for perceived violations of privacy laws. They should take all necessary steps to ensure compliance with ap-

  HITR ISSN 2151-2876

plicable HIPAA privacy and security provisions, including but not limited to the following:

- Examine their HIPAA security policies and procedures to make certain that their safeguards are adequate to prevent breaches of PHI and that their staff are adequately trained;
- Review their privacy policies and procedures to ensure that they are complete, organized, and consistent with HIPAA, the HITECH Act, and any state laws governing the organization.
- Verify that their actual practices regarding HIPAA privacy and security conform to the requirements of the written policies and procedures, and that compliance is properly documented.
- Ensure that a business associate agreement has been executed before any PHI is transferred to a business associate.

Conclusion and Implications

Although Swanson's lawsuit is the first example of a state attorney general using HITECH's new enforcement power to secure a settlement with a business associate, this case could be an indication of many such lawsuits to come.

The inclination of attorneys general in using this authority may vary from state to state, but as elected officials, some AGs are likely to be similarly aggressive in doing so.

Moreover, as this case demonstrates, a privacy enforcement investigation may reveal violations of state consumer protections and open the door to further allegations of wrongdoing. Given the high level of exposure from both a legal and public relations perspective, it is important for businesses subject to these rules to ensure their compliance with HIPAA and state privacy regulations.