Acceretive Health

On Jan. 19, 2012, in the wake of the theft of an unencrypted laptop computer containing approximately 23,500 patients' records, the Minnesota attorney general brought the first formal enforcement action against a business associate, Accretive Health, Inc., for an alleged violation under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), using her authority under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Additionally, the attorney general appears deeply unsettled by the amount of information that Accretive Health collected about patients without the patients' knowledge, alleging that this lack of transparency represents deceptive and fraudulent practices under Minnesota law.

Although the U.S. Department of Health and Human Services ("HHS") has indicated that it will not enforce the HITECH Act (such as with respect to the application of HIPAA against business associates) until the final omnibus regulation becomes effective, the Minnesota suit against Accretive Health is a reminder that the HITECH Act's statutory provisions with respect to business associates currently are in effect and that state attorneys general (as well as the U.S. Department of Justice) are not bound by HHS' enforcement discretion when considering the exercise of their authority to enforce HIPAA.

Business associates may want to review whether they currently are complying with the statutory privacy and security requirements of the HITECH Act, such as requirements to:

- Limit uses and disclosures of protected health information
- Perform and document risk analysis and risk management processes
- Implement reasonable and appropriate administrative, physical, and technical safeguards, particularly with respect to electronic protected health information
- Formalize privacy and security efforts through policies and procedures
- Appoint a security officer (and perhaps a privacy officer)
- Verify compliance with existing business associate contracts – failure to comply may result in increased liability beyond breach of contract.

Additionally, business associates should monitor this suit because the Minnesota attorney general's request for Accretive Health to affirmatively disclose to patients its collection of health information could represent a fundamental shift in the relationship between business associates and patients and may create substantial additional notification obligations and costs.

Background According to the Minnesota attorney general's complaint, Accretive has a controversial history in Minnesota with respect to its arbitration and collection of consumer debts. Accretive Health is a "portfolio company" of Accretive, LLC, which allegedly tried to create a "comprehensive, alternative legal system" for debt collection by taking a governing interest in the National Arbitration Forum (the nation's largest arbitration firm for consumer credit card collections), forming Axiant (a large national debt collection agency for the credit card industry), and acquiring the assets and collections of Mann Bracken law firm (the nation's largest collection law firm). The Minnesota attorney general filed a lawsuit against the National Arbitration Forum in 2009 for allegedly misleading consumers, and it is through this lens that the attorney general apparently viewed the activities of Accretive Health.

According to the complaint, on July 25, 2011, an Accretive Health employee allegedly left a password-protected, unencrypted laptop containing the patient information regarding two hospitals in the back seat of a rental car, where the laptop was stolen. Accretive Health provided revenue cycle management activities to the two hospitals, ranging from "front office" (scheduling, registration, and admissions), "middle office" (billing), to "back office" (collections). Additionally, with respect to one of the hospitals, Accretive Health provided "quality and total cost of care" activities, in which Accretive helped the hospital negotiate contracts with certain insurance companies in which the hospital would receive incentive payments for cutting health care costs, with Accretive receiving a portion of any incentive payments in exchange for "managing the care coordination process". Based on these activities, the stolen laptop allegedly contained names, addresses, dates of birth, social security numbers, Accretive-derived scores to predict the "complexity" and likelihood of inpatient admission of patients, and information regarding whether patients had any of 19 conditions (e.g., HIV, diabetes, schizophrenia, and depression).

Security Allegations The attorney general's complaint alleges eight security violations of HIPAA, such as a failure to implement policies and procedures to prevent, detect, contain, and correct security violations, to effectively train employees, and to implement policies regarding the receipt and removal of