BAs Beware: The Government Will Go After You for HIPAA Violations

Mindi M. Johnson

Foster Swift Health Care Law E-News
May 2012

AUTHORS/ CONTRIBUTORS
Mindi M. Johnson

PRACTICE AREAS
Health Care
HIPAA Privacy & Security Compliance

In a recent complaint filed in Minnesota against Accretive Health, a business associate was implicated for breach of the Health Insurance Portability and Accountability Act ("HIPAA"). Accretive Health has assumed control of the "so called" revenue cycle operations of both Fairview Health System Services ("Fairview") and North Memorial Health Care ("North Memorial"), which includes scheduling, registration, admissions, billing, collection and payment functions. Accretive Health has assumed managerial responsibility for the hospital employees and has infused its own employees into the staff of the hospitals. It also engages in data mining and consumer behavior modeling on patients. As a result, Accretive Health has compiled a high volume of personal, medical and financial data on Fairview and North Memorial patients.

This action arose as a result of the theft of an unencrypted laptop computer left by an Accretive Health employee in a rental car outside a bar/restaurant in Minneapolis. The stolen computer contained data related to at least 23,531 patients. This action is significant because it represents one of the first instances in which a "business associate" has been sued for alleged violations of HIPAA. It also reveals the high level of scrutiny a business associate's operations may face after a data breach.

BUSINESS ASSOCIATE RELATIONSHIP WITH FAIRVIEW AND NORTH MEMORIAL

Accretive served as a Business Associate for both Fairview and North Memorial. As such, it contractually agreed that it would not use or disclose protected health information in violation of HIPAA or the Health Information Technology for Economic and Clinical Health ("HITECH") Act. It also agreed that it would use "appropriate safeguards to prevent the misuse or disclosure of protected health information."

CHARGES AGAINST ACCRETIVE HEALTH

The Minnesota Attorney General brought charges against Accretive for, among other things, violations of HIPAA. The Attorney General alleged that Accretive not only failed to properly safeguard such sensitive information, but also that it failed to keep track of the information and identities of all of the individuals whose data was exposed. Protected health information of patients that was stored on the stolen computer included names, addresses, dates of birth, Social Security numbers, other identifiers, clinical information, diagnosis and conditions, financial information, dates of service, account balances, account numbers, and medical records numbers, among other data.

Alleged HIPAA violations against Accretive include failure to:

- implement policies and procedures to prevent, detect, contain, and correct security violations;
- implement policies and procedures to ensure 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 such access;
- effectively train all members of its workforce, including agents and independent contractors involved in a data breach, on the policies and procedures with respect to protected health information;
- identify and respond to suspected or known security incidents and to mitigate the same;
- implement policies and procedures to limit physical access to electronic information;
- implement policies governing the receipt and removal of hardware and electronic media that contain electronic protected health information;
- implement technical policies and procedures for electronic information systems that maintain electronic protected health information; and
- implement reasonable and appropriate policies and procedures to comply with the legal requirements.

RELIEF REQUESTED

Overall, the Minnesota Attorney General requested that Accretive stop violating federal health privacy laws, state privacy laws and state consumer protection laws; pay statutory damages for all violations; pay plaintiff's costs in the action; and disclose to Minnesota patients the data it has about them, where and how such data is stored, and how such data is utilized.

CONCLUSION

As indicated, this case reveals the extent of potential liability faced by a Business Associate in the event of a data breach. It also discloses the level of exposure to which the Business Associate's operations may be subjected. When organizations begin working with a health care provider and using protected health information, they must ensure a clear Business Associate agreement is in place. They should also take affirmative steps to fully implement the provisions of such an agreement. It would also be prudent to analyze their operations under the relevant Michigan laws related to privacy and release of medical records to ensure ongoing compliance. If you have any questions about these issues or would like our assistance in addressing them, please do not hesitate to contact a Foster Swift Health Care attorney.