Bond

INFORMATION MEMO
HEALTH CARE LAW

DECEMBER 2015

HIPAA Covered Entities: Your Organization's Liability after a Cyber-Attack

It is difficult for companies to manage the rapidly evolving legal landscape of cybersecurity. All companies, no matter the size, are potential targets for a cyber-attack. A common question posed by concerned In-House Attorneys, Chief Executive Officers, Chief Information Officers, and Risk Managers is – what types of lawsuits might we be forced to defend if our company is 'hacked'? This concern is magnified for organizations covered by the Health Insurance Portability and Accountability Act (HIPAA) and their business associates due to HIPAA breach requirements and regulatory oversight.

On November 15, 2015, a Florida Federal Judge entered an Order providing valuable insight as to what legal claims may be brought against a company after a data breach occurs, and whether those claims can be based on alleged HIPAA violations. In *Yehonatan Weinberg v. Advanced Data Processing, Inc., et. al.*, Mr. Weinberg, individually and on behalf of a class, asserted claims of negligence, breach of fiduciary duty, and unjust enrichment against Advanced Data Processing and Intermedix Corp. (doing business collectively as Intermedix). Intermedix is a data processing company and health care payment processor. Allegedly, in 2012 an Intermedix employee accessed and viewed a large number patients' personal information and used that information to steal identities. In Florida, as in New York State, a data breach is defined as the unauthorized access to data in electronic form containing personal information.

The Federal Judge ruled that Mr. Weinberg could bring a cause of action against Intermedix for (1) negligence and (2) unjust enrichment. However, the Court dismissed Mr. Weinberg's claim for breach of fiduciary duty. The Court reasoned that Mr. Weinberg's could pursue his negligence claim against Intermedix under Florida's "undertaker's doctrine." This theory provides that a person voluntarily or contractually providing services to others has a duty to act carefully. Intermedix's duty, however, did not extend so far as to create a duty that would be recognized in a claim for breach of fiduciary duty. Ultimately, the Court found that the mere receipt of confidential information was insufficient by itself to transform an arm's length transaction into a fiduciary relationship between the parties that could give rise to a breach of fiduciary duty claim.

Although the Court allowed Mr. Weinberg to pursue his claim for negligence under Florida's "undertaker's doctrine," it ruled that HIPAA did not provide the basis for Mr. Weinberg's claims. The Court reasoned that HIPAA does not provide a private right of action. Because prior courts refused to recognize a private right of action for negligence per se based on an alleged violation of federal statute where the statute does not provide for a private right of action, the Federal Judge did not allow Mr. Weinberg's claim of negligence to be based upon an alleged violation of HIPAA.

However, other courts have permitted a private cause of action to proceed under HIPAA for the improper disclosure of protected health information (*e.g.*, invasion of privacy, breach of confidentiality, negligence, and infliction of emotional distress) resulting from a cyber-attack. As the cybersecurity legal landscape evolves, Plaintiff's attorneys are likely to seek new causes of action under HIPAA and otherwise. In addition, many states have adopted laws requiring notice to individuals whose private information in the form of a social security number, credit card information, or other personal data has been hacked.

Entities covered by HIPAA (Covered Entities) must report all breaches of protected health information annually to the United States Department of Health and Human Services (HHS). For breaches that affect more than 500 individuals, notice must be provided immediately to HHS and to media outlets, opening the door to federal and state enforcement action. HIPAA also requires Covered Entities to notify each individual whose unsecured protected health information was accessed, acquired or used as a result of the breach. The notice must include a description of what happened, the types of information affected, and any steps individuals should take to protect themselves from potential harm. Business Associates must notify the Covered Entity of any breach and cooperate in the investigation to identify the facts required for notice.

After a cyber-attack occurs, it is therefore imperative for organizations to seek advice of counsel to determine what causes of action, if any, may be brought by private parties and to ascertain the obligation to provide notice to affected individuals. Organizations that are Covered Entities under HIPAA and their Business Associates will require assistance of counsel to determine their notice obligations to HHS, to conduct an investigation to prepare the mandated notice if necessary, and to address potential government investigation and enforcement action that may follow.

Please contact Lisa A. Christensen (315.218.8279; lchristensen@bsk.com), Tracy E. Miller (646.253.2308; tmiller@bsk.com) or Thomas K. Rinaldi (239.659.3866; trinaldi@bsk.com) if you would like to discuss how your organization can proactively prepare for a breach, or if your organization has been the victim of a cyber-attack, how it can respond to the breach by addressing regulatory obligations and any claims made by customers or third-parties for the breach of personal information.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond