S.D. TEXAS: HOSPITAL CANNOT BE SUED FOR INCREASED RISK OF FUTURE HARM FROM DATA BREACH

This month's announcement of the recent Anthem Data Breach sent shockwaves through the health care industry with some experts referring to 2015 as the “year of the health care hack." Those who collect and store health data have been racing to strengthen security protocols and to understand their risk exposure. In a first-of-its-kind case in the Fifth Circuit, the Federal District Court for the Southern District of Texas determined that a patient cannot bring a claim against a hospital for the potential damages she would face as a result of a data breach that included her health information.

THE CASE

The class action lawsuit was brought by a former patient of the defendant-hospital whose information was part of a 2013 data breach of the hospital's network. The plaintiff in the case alleged violations of the Fair Credit Reporting Act (a federal statute) as well as state law claims. The plaintiff alleged of multiple incidents where her data had been used to breach her online email and shopping accounts, as well as direct solicitations to her via mail, phone and email.

Defendants moved to dismiss, arguing that these incidents present no actual damage from which the plaintiff could recover and that in fact such allegations impermissibly seek judgment for the threat of future harm.

The key question for the court was whether the Plaintiff had standing to bring a claim - that is, whether she had suffered the type of injury that permits her to bring a claim. The court found that she lacked standing for her federal claims and therefore dismissed them. Relying on cases from other federal circuits, the Plaintiff responded that the data breach put her at specific risk of "real and impending" identity fraud or theft.

THE DECISION

The Court found it had no authority to hear the plaintiff's case "unless and until" her theories of increased risk actually result in harm. Though fraud and identity theft may occur using the information gained from the breach, absent an actual incident causing her harm, there is simply no legal basis for her claim. The Plaintiff's case, the court found, is essentially one seeking relief for "future injuries" and such a basis has been roundly rejected by the Supreme Court of the United States. Importantly, the caselaw from other federal Circuits that the Plaintiff attempted to rely on had been overruled by the Supreme Court's decision in *Clapper v. Amnesty International et al.*

HEALTH CARE TAKEAWAY

Health care providers use of information is transforming the provision of health care as this innovation brings new risks and opportunities. Strategic minded providers conscious of patient privacy should proactively adopt policies to address all forms of information that are collected and stored in the clinical practice and administration of health care services. Information needing specific protections can range from financial information to patient information, to emerging “big data” operations for population health management or accountable care organizations. Forward-thinking providers should have in place strong up to date policies and contractual protections with their information technology vendors to protect all types of sensitive information, prevent security breaches and avoid unnecessary litigation.

Should you have any questions regarding health care or commercial litigation and defense against data breach claims, please contact:

- Drew B. Howk at ahowk@hallrender.com or (317) 429-3607; or
- Your regular Hall Render attorney.

Should you have any questions regarding Big Data strategies, data and cyber risk management or health care privacy and security policies, please contact:

- Your regular Hall Render attorney.