CLIENT ALERTS & INSIGHTS

Lessons Learned from the Anthem Cyber-Attack and Corresponding "HIPAA Actions"

MARCH 13, 2015

Authors: Daniel Meier

Anthem Inc. ("Anthem"), the nation's second-largest health insurer, disclosed on Wednesday, February 4, 2015, that it was the victim of a major cyber-attack. According to Anthem, the attack exposed personal information of approximately 80 million individuals, including member names, member health ID and Social Security numbers, dates of birth, addresses, telephone numbers, email addresses and employment information. As of date of this publication, it has not yet been determined whether the hackers obtained access to health information.

The day after Anthem's announcement, the first of several class action lawsuits against Anthem for the data breach was filed. Approximately 40 additional cases have since been filed against Anthem. The class actions allege harm due to the disclosure and compromise of the plaintiffs' personal, health and financial information resulting from the Anthem data breach and Anthem's purported failure to provide timely and accurate notice. Moreover, the class actions claim that Anthem did not encrypt the data that was stolen. Amongst other causes of action, the lawsuits have alleged claims for negligence, negligence per se, breach of implied contract, and violations of various state laws.

These lawsuits demonstrate that the healthcare industry should be concerned about the privacy and security of the personal, health and financial information in their possession for reasons beyond just the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d, *et seq.* ("HIPAA"). HIPAA does not provide for a private right of action. However, as explained in more detail below, several states have recently allowed plaintiffs to sidestep HIPAA's prohibition of a private right of action. Courts have allowed plaintiffs to use HIPAA to set the standard of care in state law claims, including negligence, invasion of privacy and state privacy claims.

State's Highest Court Permits Claims Premised On HIPAA's Standard of Care

Several state courts have recently permitted private claims related to HIPAA to go forward over state law. Notably, the Connecticut Supreme Court recently held that HIPAA does not preempt common-law claims for negligence and negligent infliction of emotional distress against a health care provider. In *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.,* 314 Conn. 433, 102 A.3d 32 (Conn. 2014), the court found that HIPAA may be considered in determining the standard of care governing the handling of medical records in connection with negligence claims under state law. Other courts have allowed similar claims. *See, e.g., R. K. v. St. Mary's Med. Ctr., Inc.,* 229 W. Va. 712, 718-21 (W. Va. 2012) (using HIPAA as standard of care for breach of medical confidentiality); *Acosta v. Byrum,* 180 N.C. App. 562, 568 (N.C. Ct. App. 2006) (acknowledging HIPAA as setting the standard of care); *I.S. v. Washington Univ.,* 2011 U.S. Dist. LEXIS 66043, at *16 (E.D. Mo. June 14, 2011) (recognizing claim for negligence per se despite HIPAA). However, *Byrne* is the first by a state's highest court.

In *Byrne*, defendant medical practice produced plaintiff's medical records pursuant to a subpoena in the context of a paternity suit. The practice did not notify plaintiff of the disclosure despite her directions not to release the records. *Byrne*, 314 Conn. at 437. Plaintiff then filed a lawsuit alleging that the defendant medical practice: (1) breached its contract with plaintiff by violating its privacy policy and disclosing her protected health information ("PHI") without authorization; (2) negligently failed to use proper and reasonable care in protecting her medical file; (3) negligently misrepresented that the privacy of her health information would be protected in accordance with law; and (4) engaged in conduct constituting negligent infliction of emotion distress. *Id.* at 438.

The Connecticut Supreme Court reversed the trial court's dismissal of plaintiff's tort claims by finding that state laws relating to the privacy of PHI, which are more stringent than HIPAA, are exempt from HIPAA preemption. State laws are only preempted if they are contrary to HIPAA by making it impossible to comply with both state and federal requirements or by posing as an obstacle in complying with HIPAA. Moreover, the court pointed to the regulatory intent behind HIPAA, which expressly provides that state laws allowing individuals to file civil actions to protect privacy does not conflict with HIPAA penalty provisions. *Id.* at 454. The *Byrne* court concluded that HIPAA and its implementing regulations can be used to inform the standard of care applicable to state law claims arising from allegations of negligence in the disclosure of a patient's medical records.

Ultimately, the Connecticut Supreme Court sent the case back to the trial court for further proceedings. The trial court still has to determine whether the defendant medical practice's disclosure of the patient's medical records was negligent, constituted negligent infliction of emotional distress, involved negligent misrepresentation of the records' privacy protections, or was a breach of contract with the patient due violations of privacy policies. Based on the Supreme Court's decision, the trial court can now use HIPAA as the standard to decide these causes of action.

Court's Failure to Consider the Distinction Between "Required" and "Addressable" safeguards

The *Byrne* case was significant for being the highest court in a state to hold that Covered Entities and Business Associates could be liable under common law for their failure to comply with HIPAA. However, the *Byrne* case is also concerning due to its failure to distinguish between HIPAA's "required" and "addressable" safeguards. As explained by the U.S. Department of Health & Human Service's Office of Civil rights ("OCR"), some safeguard implementations are "required" and others are "addressable."

Required implementation specifications must be implemented. http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html (last visited February 15, 2015). However, "addressable implementation specifications" must be implemented if it is a reasonable and appropriate security measure to apply within its particular security framework. Accordingly, addressable safeguards provide companies with some flexibility in complying with security standards. The decision will be based on a number of factors such as, "the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation." *Id.*

Given that the *Byrne* court did not address the safeguard distinction, it is unclear whether a company that does implement an addressable safeguard under HIPAA, such as encrypting, would fall below the standard of care for state law claims. As mentioned above, the actions against Anthem assert that Anthem failed to implement appropriate encryption measures to secure its data. Whether this

failure meets or falls below the standard of care may determine whether Anthem is found liable of any of the state law claims.

Due to the ambiguity in the *Byrne* decision, companies should consider their exposure and risks in connection with implementing both "required" and "addressable" safeguards.

First Case With Substantial Damages Premised On HIPAA's Standard of Care

In another major case that broadened the exposure to Covered Entities and Business Associates, on November 14, 2014, the Court of Appeals of Indiana affirmed a $1.44 million judgment against Walgreen Company ("Walgreen") based on a HIPAA violation. *Walgreen Co. v. Hinchy*, 21 N.E.3d 99, 2014 Ind. App. LEXIS 560 (Ind. Ct. App. Nov. 14, 2014). Equally notable is that the court held that the employer is subject to vicarious liability for state negligence claims stemming from a HIPAA violation committed by an employee.

In *Walgreen*, Defendant Withers a pharmacist at Walgreens, learned that her husband had been having an affair with plaintiff, which resulted in the birth of a child. Defendant Withers accessed plaintiff's patient information through the Walgreen's computer system, reviewed plaintiff's prescription history for personal reasons and disclosed this history to her husband. Upon learning of the incident, Walgreen gave defendant Withers a written warning and required her to retake a computer HIPAA training program. Plaintiff was dissatisfied and sued Withers with claims of negligence/professional malpractice, invasion of privacy/public disclosure of private facts, and invasion of privacy/intrusion. Plaintiff also filed claims against Walgreen to hold them responsible for the actions of the employee, as well as direct claims for negligent training, negligent supervision, negligent retention, and negligence/professional malpractice. Essentially, plaintiff claimed that defendant Withers' and Walgreen's actions fell below the standard of care provided by HIPAA. The jury found for plaintiff and awarded her $1.44 million in damages, which notably included damages for emotional distress.

Conclusion

As demonstrated above and through the Anthem class actions, not only are Covered Entities and Business Associates now at risk due to OCR enforcement, but they must also be wary of state claims premised upon HIPAA regulations. The *Byrne and Walgreen* decisions allowed plaintiffs to use HIPAA to help determine the standard of care with respect to the duty to maintain confidentiality. Covered Entities and Business Associates should revisit their policies and procedures to ensure compliance with HIPAA's privacy and security standards. Importantly, Walgreen was also found to be vicariously liable for its employee's actions since the records were accessed under the scope of defendant's employment. Accordingly, it is vital for Covered Entities, Business Associates and subcontractors to evaluate their privacy and security policies and programs to ensure compliance with HIPAA.

The lawsuits arising from the Anthem cyber-attack serve as a reminder to healthcare companies to be diligent about protecting against security and privacy risks. In particular, security compliance requires reassessments on a regular basis. There are many healthcare companies who have not reexamined their security practices and are ripe for such an attack and potential breach. To prevent such injuries, it is imperative to not only establish but also reevaluate a security infrastructure that will meet cybersecurity requirements (including HIPAA security and privacy).

For more information on the Anthem class action, private causes of action related to HIPAA or implementation of HIPAA privacy and security policies, please feel free to contact Daniel Meier, Clifford Mull or any member of Benesch's Health Care Practice Group for a further discussion.