



Patient Privacy Breach... All in a Day's Work?

04.12.2019

It is a health care provider's nightmare ? despite extensive HIPAA training and best efforts to hire the right people, one of your staff members has gone rogue with a patient's information. Whether a receptionist loudly comments on health information in a full waiting room, or a nurse surreptitiously looks up his ex-girlfriend's health history, a provider may be liable in certain circumstances for the careless, or downright inappropriate, use and disclosure of a patient's health information.

In Virginia, patients' medical information receives privacy protection under (1) tort law, which provides for civil damages; and (2) state and federal privacy statutes, violations of which may result in civil penalties. However, the measures that health care providers should take to eliminate or reduce their liability exposure are very much the same under both regimes. The provider who prioritizes HIPAA compliance is also simultaneously accounting for state privacy law compliance. The Supreme Court of Virginia has recently weighed in on the matter, in a case that is instructive for providers who are concerned with protecting patient medical information in the hands of their employees.

In Parker v. Carilion Clinic, Virginia's highest court partially revived a lawsuit against a health care provider and its two employees for allegedly disclosing confidential patient information. In her complaint, the plaintiff, Lindsey Parker, alleged that Carilion Clinic and Carilion Healthcare Corporation (hereinafter "Carilion") and two employees, Christy Davis and Lindsey Young, unlawfully disclosed Ms. Parker's confidential medical information to an unauthorized acquaintance.[1] Parker alleged that seven months after she was diagnosed with a medical condition at a Carilion-owned OB-GYN, she was awaiting treatment at a Carilion-owned family medicine clinic when she struck up a conversation with a male acquaintance. Davis, who also knew the man, witnessed the conversation in the waiting room and pulled up Parker's medical file. After seeing the OB-GYN diagnosis in Parker's file, Davis called Young, Davis's friend and fellow Carilion employee. Davis relayed to Young information regarding Parker's diagnosis and that Parker was conversing with the man whom they all knew. The plaintiff alleged that Young then disclosed Parker's diagnosis to the man without Parker's authorization. The man, in turn, told Parker about what he had heard.[2]

The Supreme Court determined that the clinic could be found vicariously liable for the unauthorized disclosures of medical information made by its employees because the employees *could have been* acting within the scope of their employment^[3] when the alleged disclosure occurred.^[4] The Court held that sufficient information was provided in the pleadings^[5] to establish a rebuttable presumption that the employees acted within the scope of their employment when the disclosure was made, because Carilion acknowledged that Davis and Young were in fact employees of the clinic. This presumption, if not overcome by evidence, would lead to the determination that Carilion should be held vicariously liable for the employees' actions. As such, the Court found that "facts that come to light later might affirm or disaffirm the presumption,"^[6] and, therefore, the lower court's granting of summary judgment was premature and in error.^[7]

This opinion has brought to light a pocket of legal exposure for Virginia health care providers' state law vicarious tort liability for the unauthorized disclosures of medical information by employees. This unauthorized disclosure cause of action in Virginia was defined in the 1997 Supreme Court of Virginia opinion Fairfax Hospital v. Curtis, holding that "a health care provider owes a duty to the patient not to disclose information gained from the patient during course of treatment without the patient's authorization, and violation of this duty gives rise to an action in tort."^[8] In Parker, when the lower court re-examines this issue on remand, Carilion could be found vicariously liable for disclosures made by Davis and Young under the theory of *respondeat superior* (Latin for "let the master answer").

Respondeat superior vicarious liability is frequently explained as the employer being liable for "detours" of the employee (i.e., a personal stop at the post office in a company truck out for a delivery); but not for "frolics" of the employee (i.e., stopping to catch a baseball game in a company truck that is supposed to be out for a delivery). The scope of employment analysis is paramount to determining employer liability: an employee frolic is a major departure from the charge given by the employer, and thus is outside of the scope of employment. The line between frolic and detour is fuzzy when it comes to employees with computer access, but having a clear computer use policy and employee training can help establish a more precise line. For health care providers, an employee snooping on a personal acquaintance's health information, unrelated to the treatment of a patient, could be found to be a "frolic," but the Parker opinion clarifies that this analysis will be fact-specific.

Measures taken by the employer to protect patient medical information under HIPAA are the basis for the employer's defense. If the employer demonstrates that privacy policies are monitored, and that employee violations are subject to discipline or termination, then the employer is able to mount a credible defense that the snooping employee frolicked outside of the scope of his or her employment. In such a case, a fact-specific analysis could find the employee individually liable for civil damages under Virginia tort law, without finding the employer vicariously liable for the employee's violation. The same defense would be mounted in a federal HIPAA claim against an employer for civil penalties payable to the government. Virginia privacy law and HIPAA operate independently of each other; however, the relevant

facts analyzed in questions of compliance are very similar.

In Parker, the Supreme Court dismissed the contention that Carilion could be found directly liable for unlawful disclosure. The complaint did not allege that Davis or Young were corporate officers or authorized agents acting on behalf of Carilion.[9] nor did the Court find that Carilion could be liable under a negligence *per se* theory (legal doctrine whereby an act is considered negligent because it violates a statute or regulation) that a HIPAA breach gave rise to negligence liability. The Court clarified the distinction between the aim of the Virginia tort duty not to disclose patient's medical information and the aim of the HIPAA duty to protect patient information. Even if Parker argued that a HIPAA breach occurred, there would be no parallel breach of a duty established by Virginia state law because "[n]o Virginia precedent has imposed such a tort duty on healthcare providers." [10] The Parker holding closes the door on theories of negligence *per se* liability for HIPAA violations, confirming that there is no private cause of action under HIPAA. The Court notes that the plaintiff could have pursued a direct liability claim that Carilion was negligent in hiring Davis and Young, though Parker did not raise this claim.[11]

This decision serves as a reminder that Virginia courts do not take matters of privacy lightly. In the wake of this opinion, it is important for health care providers to impose strict privacy measures, particularly with employee procedures and training. Absent a more stringent state privacy law, HIPAA compliance is the gold standard for protecting patient privacy[12] Best employer practices include:

- Keeping medical records in restricted areas and locked file cabinets, and when electronic, keeping records in restricted-access, password-protected files and programs.
- Establishing role-based access to computer systems that store sensitive and confidential information, and terminating employee access to the facility(ies) and computers when an employee has left the organization.
- Ensuring that only employees directly involved in treating patients or processing the payment or other operational tasks for such treatment should be permitted access to that patient's record.
- Turning computer screens in a direction away from the public view, and making sure passwords to computers that house medical information are changed every 90 days.
- Speaking quietly when discussing patients' medical conditions in public areas, and avoiding the use of the patients' name when necessary.
- Designating a staff member to handle privacy compliance and concerns.
- Establishing policies and procedures for accessing, sharing and securing a patient's health information including computer and internet usage, and password protecting and encrypting the transfer of medical records over electronic mail.
- Conducting frequent staff training on privacy regulations and policies regarding computer use.
- Establishing employment procedures that impose consequences (discipline and/or termination) for employees who fail to follow privacy practices.[13]

[1] Parker v. Carilion Clinic, 819 S.E.2d 809, 823 (Va. 2018).

[2] Id. at 814.

[3] The Court expounds upon the scope of employment analysis in finding vicarious liability, which is not addressed in this article. The concurring opinion by Justice Mims, with whom Justice Powell joined, differentiates the role employees' motives play in the determination of whether they acted within the scope of their employment.

[4] Id.

[5] The Supreme Court ruled upon an appeal of the Roanoke Circuit Court's grant of Carilion's demurrer (which asks the court to dismiss the complaint because it does not state an actionable legal claim). The Supreme Court found that the vicarious liability presumption can be established at the pleadings stage, and when allegations are taken as true, there was a sufficient basis to raise the presumption that the employees were acting within the scope of their employment, and the presumption had not yet been overcome.

[6] Id. at 822.

[7] The Court dismissed Carilion's argument that, even if the presumption were raised, it had been rebutted because the allegations in the plaintiff's complaint demonstrated that

the employees were *not* acting within the scope of their employment. The Court disagreed and found that the presumption arose from the allegations that Davis and Young were employees, and neither the allegations of the complaint nor any factual inferences provided a basis for refuting that presumption. See Parker 819 S.E.2d at 818.

[8] Fairfax Hosp. By & Through INOVA Health Sys. Hosps., Inc. v. Curtis, 492 S.E.2d 642, 645 (1997).

[9] Id. at 823-24

[10] Id. at 826.

[11] Id. at 826 n.15.

[12] 42 U.S.C. § 1320d-7.

[13] Office of Civil Rights, HIPAA Privacy: Incidental Uses and Disclosures (2002); see 45 C.F.R. § 164.502(a)(1)(iii); Va. Code § 32.1-127.1:03.

Related People

- Stefanie A. Felitto ? 804.420.6204 ? sfelitto@williamsmullen.com
- Rebecca E. Ivey ? 804.420.6334 ? rivey@williamsmullen.com