Patients Can Sue in State Court for Confidentiality/Privacy Breaches Despite HIPAA

Earlier this month, the Connecticut Supreme Court concluded in *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.* that a patient could sue her former OB-GYN physician practice in state court for improperly disclosing her records, despite the fact that HIPAA does not permit individuals to sue for HIPAA violations. Prior to this decision, courts generally dismissed state law claims that essentially alleged a HIPAA violation because HIPAA did not allow private lawsuits. Not only are these claims now permitted, but the patient may also use the HIPAA regulations to show how providers should be ensuring privacy and confidentiality of health records.

Due to the procedural status of the case, the facts are not well-developed. The limited available facts, however, reveal that an OB-GYN practice received a subpoena for the records of a former patient who was involved in a paternity case filed by an ex-boyfriend. In response to the subpoena, the practice mailed a copy of the former patient's medical file to court. The practice contends that the court staff failed to seal the records pending a court order and instead placed the records in the court file without a court order. The patient claims that after the ex-boyfriend saw the records, he began harassing and threatening her. She sued the OB-GYN practice for negligence and negligent infliction of emotional distress, as well as breach of contract and negligent misrepresentation based on the Notice of Privacy Practices.

The trial court dismissed the negligence and negligent infliction of emotional distress claims, ruling that they were preempted by HIPAA, but the state Supreme Court disagreed. The Court explained that any state law that protects the privacy and confidentiality of medical records is not contrary to HIPAA and, as a result, permitting a patient to sue the practice under state law is not at odds with the spirit of HIPAA.

In addition to allowing the patient to pursue her negligence claims in state court, the Court went one step further in acknowledging that the HIPAA regulations could be used to establish the standard of care for the provider in that case. This ultimately means that if the provider did not comply with HIPAA requirements, that failure can be used as proof that it acted negligently in the lawsuit brought by the patient.

Similarly, this summer, a superior court permitted a lawsuit related to electronic access of medical records in *Emslie v. Craig*. The court in that case held that HIPAA did not block a lawsuit by an individual for improper use and access of medical records on a computer system under Conn. Gen. Stat. § 53-251 because that claim was rooted in the plain language of the statute, regardless of HIPAA. The plaintiff in that case asserted that the doctor took advantage of his position as a licensed physician to wrongfully access confidential information on Danbury Hospital’s computer system.
Because both of these cases were at the preliminary stages of litigation, the facts have not been fully developed and ultimate liability issues have not been determined. These decisions, however, highlight the importance of complying with state and federal privacy and confidentiality laws. In particular, the Byrne case underscores the fact that a failure to comply with HIPAA may subject providers to lawsuits in state court. But just as critically, the reverse is also true – compliance with HIPAA will help a provider prove that he or she acted properly and help avoid liability.

The other two claims in Byrne, breach of contract and negligent misrepresentation, which are both based on the Notice of Privacy practices, are also worth mentioning. Providers should be aware that they will be held responsible for acting in a manner that is consistent with their Notice of Privacy Practices. In order to minimize the risk of a lawsuit by a patient for a confidentiality breach, providers should not only comply with federal and state law but they must also adhere to their own Notice of Privacy Practices.

Byrne also reminds us that subpoena compliance can be challenging. Under very limited circumstances, it is possible to comply with a subpoena request when there is no authorization, but in light of this case, providers may decide to insist on an authorization or court order prior to providing records.

As a final note, providers may want to consider having new patients consent to alternative dispute resolution. Such a clause could require informal discussion with the privacy officer, formal mediation, and then arbitration. It might also prohibit class actions and possibly limit damages. Providers interested in seeking patient consent for alternative dispute resolution are encouraged to consult with counsel as there may be enforceability concerns that must be addressed.

Providers with questions about these cases or compliance with state or federal confidentiality or privacy laws should contact Dena M. Castricone at (203) 772-7767 or dcastricone@murthalaw.com or Stephanie Sprague Sobkowiak at (203) 772-7782 or ssobkowiak@murthalaw.com.