MYTH: A patient may sue a provider in federal court under HIPAA for an unauthorized disclosure of their health information.

FACT: HIPAA provides no right to sue for violations in court. Complaints may be filed with the Office of Civil Rights within the Department of Health and Human Services and the applicable State Attorney General, who will then investigate and enforce the law.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule regulates the use and disclosure of patients' protected health information (PHI) by covered entities and business associates that hold such data. When a patient's PHI is used or released without their consent, they naturally may wonder who they can sue for a remedy. The HIPAA Privacy Rule does not contain what is known as a "private right of action," meaning that unlike some other federal laws (such as the ADA or ERISA), the patient cannot sue in federal court for a HIPAA violation. This is because the law does not expressly provide for private enforcement and the courts, in hundreds of cases, have said no private right of action exists under HIPAA.

Therefore, the only remedy for patients alleging a HIPAA Privacy Rule violation is to file an official complaint with the Office of Civil Rights within the Department of Health and Human Services. This agency has the discretion to investigate the complaint and file a federal civil complaint against the covered entity or business associate, if warranted. If the HIPAA violation is proven, the violator may have to pay a penalty between $100 per violation (up to $25,000 total per year) to $50,000 per violation (up to $1.5 million total per year), depending on the nature and extent of both the violation and the harm it caused.

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[1] made two significant changes to the HIPAA Privacy Rule enforcement scheme. First, state attorneys general are now authorized to bring civil actions against HIPAA violators if the attorney general has reason to believe that the violation threatens or adversely affects any resident of the state. (Prior to HITECH, HHS was the sole enforcement agency for civil violations of HIPAA.) Second, HITECH authorized some share in monetary penalties or settlements for patients who file complaints, although the methodology to determine how that payment will be shared has not yet been developed. HHS has indicated that question will be answered in future rulemaking.

While the law is clear that a patient may not bring a federal lawsuit for a HIPAA violation, states may grant a right to sue for an equivalent violation under a state statute. For example, some states give individuals a right to sue if they are denied access to their own medical records, one of the rights granted by HIPAA. See here for a comparative map illustrating those state laws.

A patient may also sue under common law by making claims such as negligence, invasion of the right to privacy, and infliction of emotional distress. Such claims are unlikely to be successful, however, unless the patient suffered substantial, provable damage as a result of the breach.

For More Information:

- Learn about state and federal laws related to privacy.
- Read our overview of HIPAA and related resources.

Follow us on Twitter at @HealthInfoLaw

[1] 42 U.S.C. § 17930, et seq.