LAWYER LOOKOUT

HIPAA Right of Access: Six Ways to Land in Hot Water

The federal government has become laser-focused on ensuring individuals' timely access to their health records. Learn how health care practices trigger complaints that bring costly fines, bad publicity and ongoing government scrutiny.

The Health Insurance Portability and Accountability Act (HIPAA) is most widely known for its directives to keep patient information closely held and secure. However, a less-discussed aspect of HIPAA's Privacy Rule centers around providers' responsibility to provide patients access to their own health information: Right of Access standards.

HIPAA Right of Access provisions include detailed requirements for health care providers when a patient asks for health records. In such situations, what are your obligations? Do you have discretion regarding the release of information?

To help you understand, let's look at six types of HIPAA Right of Access violations.

Not Providing Timely Access

A patient's request for copies of their records, or a request that the record be provided to another practice, is an "access request." HIPAA requires that health care practices respond to a patient's access request within 30 days of receiving the request. If possible, respond sooner — and acknowledge receipt of their request.

What if the information is archived offsite or not readily accessible? If you cannot provide access within 30 calendar days, you may get up to a 30-day extension to respond. But that extension isn't automatic: you must first inform the patient of the reasons for the delay in writing. You must also confirm the date by which you'll fulfill their request. HIPAA allows you only one extension per access request.

Denying Access to the Patient

Under certain limited circumstances, a practice can deny an individual's request for access to all or some of the requested records. Depending upon the reason for the denial, the patient may have the right to have the denial reviewed by another licensed health care professional. HIPAA's regulations explain when a denial may be proper and under what circumstances a denial is reviewable.

You may not require an individual to provide a reason for requesting access. Moreover, if shared with the practice, the individual's rationale for requesting the records is not a permissible reason to deny access.

Practices are also responsible for responding to access requests where the records are maintained by one of the practice's business associates. For instance, if your electronic health records vendor maintains your records or your files are housed at an offsite records storage facility, you're still obligated to deliver those records to the patient.

Furthermore, even if you have grounds to deny access to some PHI, you must give the patient access to any other PHI requested. The challenges posed by needing to segregate and review the patient's PHI do not excuse your obligation to provide access to the portions of the record to which the patient is entitled.

Failing to Provide Access to Personal Representatives

A patient's representative has the same right of access as the patient. An individual's personal representative is typically someone who is allowed, under state law, to make health care decisions for that individual. The representative has the right to access the individual's PHI and can instruct the practice to send a copy of the PHI to another person or practice.

Not Providing Access in the Requested Format

The Privacy Rule requires you to give patients access to their records in the form and format requested if it's readily producible in that form and format. If that isn't possible, then it must be produced in a readable hard copy form or another format upon which parties agree.

You're not required to purchase new software or equipment to accommodate every possible individual request. While you must be able to provide some electronic form of records that are maintained electronically, if the patient refuses to accept the type of electronic formats you're capable of producing, you can instead provide a readable hard copy record.

Failing to Send Records to a Third Party

A patient has a right to request that a practice send their records directly to another person or entity, such as a law firm, social service agency or another medical office. To clarify some of the requirements surrounding PHI-sharing among a patient's providers, the U.S. Department of Health and Human Services (HHS) has created a PDF fact sheet titled, **Permitted Uses and Disclosures: Exchange for Health Care Operations**.

Charging Excessive Fees

HIPAA allows practices to charge a reasonable, cost-based fee for producing copies of patient records. The law's "patient rate" provision allows you to charge a fee of no more than $6.50 or a "reasonable, cost-based fee" that's based on the labor, supplies, postage and preparation of the information itself.

You must inform the patient of the fee in advance, and the fee may not include costs associated with:

- Verification.
- Documentation.
- Searching for and retrieving the PHI.
- Maintaining systems.
- Recouping capital for data access.
- Storage.
- Infrastructure.
- Other expenses not listed above, even if state law authorizes such costs.

Finally, you cannot charge a fee if you're fulfilling a patient's request using your EHR system's View, Download or Transmit functions.

State Right of Access Laws

When state laws give individuals greater rights of access to their records than the Privacy Rule, practices should follow state law. For example, HIPAA would not "preempt" (override) a state law that requires health care practices to give patients one free copy of their medical records, even though the federal law permits the provider to charge a fee. In such a situation, practices must comply with state law and provide a free copy.

However, when state laws undermine the Privacy Rule access provisions – such as one that prohibits certain laboratories from disclosing test reports directly to an individual – they are usually preempted by HIPAA and thus unenforceable.

Connor D. Jackson, JD

Connor D. Jackson is the Principal Partner at Jackson LLP, a health care law firm based in Chicago. Jackson LLP focuses on helping independent medical practices with regulatory compliance, business startup, insurance audits, contracts, employment and telehealth in CA, IL, MI, NY, TX, WI, VT and DC. Visit his firm's website at *JacksonLLP.com*.

The Costs of Non-Compliance

HHS wants to send a clear message: The price tag of a settlement far outweighs the cost of compliance, both in dollars and effort.

Settlements have ranged from $3,500 to $200,000, with an average of $70,650 in 2021 — and monetary settlements are only the beginning. Corrective action plans – which may include updated policies and procedures, increased training, and enhanced oversight – can be onerous for small practices. Inevitably, corrective action plans are far more cumbersome than routine compliance efforts.

The bottom line: every practice should develop a formal HIPAA plan that addresses patients' rights to access their health information. On an ongoing basis, monitor internal procedures and review (and enforce) your policies to ensure you reach and maintain compliance.

This article is made for educational purposes and is not intended to be specific legal advice to any particular person. It does not create an attorney-client relationship between our firm and the reader. It should not be used as a substitute for competent legal advice from a licensed attorney in your jurisdiction.