

Think Before You Click: Why Five Seconds of Curiosity Can Cost a Physician a Career

By: Laith Quasem, Esq.

Introduction

When my firm first asked me to prepare a white paper for this conference, I found myself considering no shortage of topics. Healthcare is among the most heavily regulated industries in the country, and there is certainly no shortage of legal issues affecting physicians today. I considered writing about audits, medical board proceedings, False Claims Act investigations, healthcare fraud, the Controlled Substances Act, and the increasingly complex regulatory landscape physicians navigate every day.

Instead, yet another physician-client reminded me that sometimes the most significant legal problems arise from the simplest decisions. Specifically, it reminded me how easily physicians can underestimate the legal and professional consequences of something as routine as accessing an electronic medical record without a legitimate treatment, payment, or healthcare operations purpose. In an era where virtually every patient encounter begins with the click of a mouse, it is easy to forget that every click leaves a footprint—and not every chart is yours to open.

That may sound elementary. In fact, some of you may already be thinking, *“Of course. Every physician knows not to access a patient’s medical record without a legitimate reason.”*

While I hope that’s true, the unfortunate reality is that despite annual HIPAA training, mandatory compliance modules, and institutional policies that leave little room for misunderstanding, I continue to represent physicians whose careers have been placed at risk because they accessed a medical record they simply had no business accessing. In my experience, these cases rarely involve physicians who set out to exploit protected health information for personal gain or to intentionally harm a patient. More often, they involved otherwise well-intentioned physicians whose curiosity momentarily got the better of their judgment.

A colleague was unexpectedly admitted to the hospital. A physician down the hall suddenly stopped coming to work. Someone mentioned that a well-known community member had become a patient. A rumor began circulating about a difficult case. The chart was only a few clicks away.

That moment of curiosity became a compliance investigation.

If this paper accomplishes only one thing, I hope it serves as another reminder that physicians cannot hear often enough: just because you *can* access a medical record does not mean you *should*.

Although much of my practice focuses on complex healthcare regulatory matters, licensing defense, and white collar investigations, I continue to be struck by how often significant professional consequences arise from something as straightforward as accessing a medical record without authorization—which is *entirely* preventable.

“I didn’t tell anyone.”

One misconception I occasionally encounter is the belief that merely opening a patient's chart, without printing, downloading, or sharing information, is relatively harmless. Physicians sometimes reason that if they never disclosed the information to anyone else, no real harm was done.

Unfortunately, modern electronic medical record systems do not work that way. Healthcare organizations maintain sophisticated audit capabilities. Every interaction with the electronic medical record generates a footprint that can identify who accessed a patient's record, whether the attempted access was successful, when the access occurred (often down to the second), where the access originated, which portions of the chart were viewed, and what actions were taken while inside the record. Each access event is typically assigned its own unique audit entry, allowing compliance personnel to reconstruct a user's activity with remarkable precision.

HIPAA is not limited to the disclosure of protected health information. Unauthorized access *itself* violates federal privacy requirements, employer policies, and institutional compliance standards, even if the information never leaves the computer screen. In other words, sometimes the problem is not what you did with the information. Sometimes the problem is that you looked at it at all.

Curiosity is human. The audit log is forever.

Healthcare is a uniquely personal profession. Every day, physicians encounter patients with rare diagnoses, unusually complex presentations, or conditions that naturally pique their intellectual curiosity. They also care for friends, neighbors, coworkers, fellow physicians, and, on occasion, public figures. It is therefore entirely understandable that curiosity may arise. The law, however, does not ask whether your curiosity was understandable. It asks whether your access was authorized.

Every unauthorized access case has its own facts. Whatever the reason for accessing a chart, electronic medical records have excellent memories. Compliance departments do not need eyewitnesses. More often than not, they only need the audit log.

The consequences frequently extend beyond HIPAA.

When physicians hear the phrase "HIPAA violation," many understandably think of additional compliance education or mandatory retraining.

The reality is often considerably more serious.

Depending upon the circumstances, unauthorized access to protected health information may result in:

- Internal compliance investigations;
- Written disciplinary action;
- Suspension or termination of employment;
- Medical staff investigations;
- Credentialing consequences;

- State licensing board investigations;
- Civil monetary penalties in appropriate cases; and
- Significant professional and reputational harm.

Depending on the disciplinary action ultimately imposed, additional reporting obligations under separate regulatory frameworks may also arise.

None of these outcomes is automatic. Every case turns on its own facts, the physician's intent, the extent of the access, institutional policies, and numerous other considerations.

The point is not that every unauthorized access case ends badly. Rather, it is that every instance of intentional unauthorized access is entirely preventable and carries consequences that far exceed whatever momentary curiosity prompted it in the first place.

In rare cases, the consequences become criminal.

Fortunately, criminal prosecution remains the exception rather than the rule. Nevertheless, physicians should not assume that unauthorized access to protected health information is “only” an employment issue.

Congress enacted criminal penalties for certain knowing violations of HIPAA. Federal prosecutors have relied on those provisions in cases involving unauthorized access to patient information, particularly where the facts demonstrated repeated misconduct, improper motives, disclosure of protected information, or other aggravating circumstances.

Perhaps most notably, in *United States v. Zhou*, 678 F.3d 1110 (9th Cir. 2012), the Ninth Circuit affirmed the criminal conviction of a former UCLA Health System employee who repeatedly accessed patient records without authorization after his employment ended. On appeal, Zhou argued that he could be convicted only if he knew that his unauthorized access violated HIPAA. The Ninth Circuit rejected that argument, holding that the term “knowingly” requires only proof that the defendant knew the facts constituting the offense—not that he knew his conduct was unlawful. As the court explained, “‘knowingly’ merely requires proof of knowledge of the facts that constitute the offense, not a culpable state of mind or knowledge of the law.” *Id.* at 1114.

For physicians, the takeaway is this: “I didn’t know it was illegal” is unlikely to be a successful defense if the evidence establishes that the access itself was intentional and unauthorized. Moreover, HIPAA’s criminal provisions are not limited to the subsequent use or disclosure of protected health information. The statute separately prohibits the knowing acquisition of individually identifiable health information in violation of HIPAA. Accordingly, in appropriate circumstances, the unauthorized access itself may be sufficient to give rise to criminal liability.

To be clear, the vast majority of physicians who improperly access a patient’s medical record will never face criminal prosecution. *Zhou* involved repeated access following the defendant’s termination from employment and is not representative of the typical workplace compliance matter. Nevertheless, it serves

as an important reminder that the law treats unauthorized access to protected health information far more seriously than many healthcare professionals appreciate.

Four questions worth asking before opening any chart.

Whenever you find yourself considering whether to access a patient's record, pause briefly and ask yourself four simple questions:

1. Am I involved in this patient's treatment, payment, or healthcare operations?
2. If Compliance reviewed this access tomorrow morning, could I clearly articulate my legitimate reason for opening this chart?
3. Would I be comfortable explaining this access to my department chair, hospital counsel, or state licensing board?
4. If I cannot confidently answer "yes" to each of these questions, why am I clicking?

Just a few seconds of reflection may save months, or years, of professional difficulty.

Final thoughts

One of the recurring themes in my practice is that physicians often assume the greatest legal risks arise from complicated regulatory schemes. More often than many realize, however, significant professional consequences arise from remarkably simple decisions made in a matter of seconds.

The overwhelming majority of physicians are ethical professionals who work extraordinarily hard to provide excellent patient care. That is precisely why this topic deserves repeating.

Annual compliance training should not be viewed as another box to check. It should serve as a reminder that professionalism extends beyond the bedside and into every interaction with the electronic medical record.

Electronic medical records have made patient information more accessible than ever before. They have also made accountability easier than ever before.

The next time curiosity gets the better of you, remember to *think before you click.*