



Who Owns Patient Medical Records?

■ K ROYAL, JD

Urgent message: While historically there has been an understanding that patients own the information contained in their records, and that providers own the record itself, lack of a federal law governing the ownership of medical records poses a conundrum when those records are stored electronically.

New challenges demand innovative solutions—often new technologies that make life easier. Certainly technology has advanced healthcare to improve our lives. Yet, perhaps more noticeable in the medical realm than in other fields, we see the clash of technology with standard practices.

Medical records are a prime example. For centuries, medical professionals have kept records on their patients. “If it’s not written, it didn’t happen” is an age-old saying in the healthcare field for a valid reason. Often, unless something was documented, no one could *prove* it happened (critical to insurance claims and lawsuits); even more importantly, however, few could *remember* what happened—what symptoms occurred when, what treatment was given and either succeeded or failed, what side effects were seen, how fast a disease spread, and numerous other critical pieces of information.

One would think that the advent of technology would make medical recordkeeping easier—and in some ways, it has. Ready availability of histories and information pertaining to medications and allergies has helped make transmitting prescriptions from the doctor’s office to the pharmacy, sending records to a specialist from the referring doctor, and receiving critical information in a timely manner commonplace. The Centers for Medicare and Medicaid Services (CMS) states that electronic health records (EHRs) “are the next step in the continued

progress of healthcare that can strengthen the relationship between patients and clinicians. The data, and the timeliness and availability of it, will enable providers to make better decisions and provide better care.”¹ The agency goes on to describe the EHR as “an electronic version of a patient’s medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person’s care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates access to information and has the potential to streamline the clinician’s workflow. The EHR also has the ability to support other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting.”¹

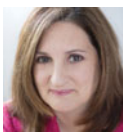
Clearly, the EHR manifests in a variety of forms and sophistication, from the simplest scanning of documents into a computer so they can be stored easily and retained, to the most complex system involving federal agencies, vendors, data crunchers, and automation for metrics, audits, and manipulation.

And therein lies our problem.

An Evolving Answer

Historically, individuals have truly *owned* their medical information. It’s a simple view; the information is about a person so, therefore, it belongs to that person. However, medical practitioners also have a huge stake in the record, because it documents what treatments were ordered and provided, and what tests were given, reviewed, and used in order to make a diagnosis or rule out a potential issue. Over time, the practical view has been that the patient owns the information, but the medical professionals—the doctors, in particular—own the records. And if a doctor works for a healthcare entity, then there is the added consideration of whether the entity has an ownership interest in the record (which they certainly do).

The U.S. does not have a federal law that states who owns medical records, although it is clear under the Health Insurance



K Royal, JD is a healthcare privacy attorney based in Scottsdale, AZ.

Portability and Accountability Act (HIPAA) that patients own their information within medical records with a few exceptions. Thus, we look to state law. New Hampshire is the only state that provides for ownership²—and even then, limits it to the information within the record: “All medical information contained in the medical records in the possession of any health-care provider is the property of the patient.” It then goes on to state that the patient has the right to receive a copy.

One could easily argue, then, that the record is not owned by the patient if the patient can only receive a copy.

Twenty states are clear that the medical records belong to either the provider or the facilities.³ This provides for an interesting debate between a provider and a facility. In the overwhelming majority of those 20 states, the facility or employer owns the records created by a provider. From a legal viewpoint, the providers would be entitled to copies, given the professional nature of the records. However, in the remaining 29 states (or 30 if we count the District of Columbia), there is no mention of ownership. According to a poll by *Medical Economics*, 33% believe patients own records, 65% believe physicians do, and 2% believe EHR vendors do.⁴

What EHR vendors own medical records? Vendors that offer

EHR systems stored remotely and offered as a cloud-based services. And wither within the same vendor or as a partner, there are analysts who review the EHRs for a variety of metrics and data points related to population health, diseases, payments, certain tests, etc. This analysis may or may not be known to the doctors or the healthcare entity. This analysis is legal and, in some ways, even encouraged to better inform the medical field in general. For example, the U.S. Centers for Disease Control and Prevention has an interest in reactions to vaccines and may track vaccines across the nation by control number, age of patient, reaction, etc.

Many healthcare providers are familiar with EHR vendors, such as Allscripts and Practice Fusion (and many others). However, EHRs also comprise those records with affiliated services, such as radiology, pharmacy, medical device manufacturers, and care coordinators. In some cases, the records with the affiliated services may be the only detailed record in existence. This can add complications for both the providers and the patients.

Denying Access

In reviewing some of the publicly available information from EHR vendors, there were some common themes, mainly around limitation of liability and access rights. In many cases,

URGENT CARE CLINIC

Medical Professional Liability Insurance

KEEP YOUR BUSINESS HEALTHY, WEALTHY AND WISE.

Let's work together to reduce your expenses with quality coverage custom-built just for you.

YOU TAKE CARE OF YOUR PATIENTS. WE'LL TAKE CARE OF YOUR RISK.

Medical malpractice insurance is essential, but finding the best policy – one that provides the proper liability protection you need at an affordable price – can be confusing.

At NFP, we take the time to answer all of your questions and make sure you select a strong, reputable and financially stable insurance policy that provides the right protection when you need it most.

As one of the largest sources to arrange insurance for urgent care clinics, our team provides:

- Per-visit rating (type and number)
- Exceptional service standards
- Prior acts coverage
- Knowledgeable, friendly staff
- Defense outside the limit
- Risk management/ educational support
- Fast turnaround on policy changes
- Exclusive “best practices” discounts
- Rapid response claim service

COMMERCIAL INSURANCE | CORPORATE BENEFITS | PRIVATE CLIENT RESOURCES

Looking for expert medical risk management? Get in touch with David Wood at 800-695-0219, Ext. 44526, or david.wood@nfp.com.

NFP.com
 (17-FCI-PGL-SW-0296) Insurance services provided through NFP Healthcare Industry Insurance Services, Inc., an affiliate of NFP Corp. (NFP). CA license #0763921.



access to the EHR can be immediately discontinued upon non-payment, allegations of misuse, or in their “sole discretion” if someone with access may jeopardize the confidentiality; may violate the agreement (note “may” not “is” or “has”); and/or violate someone’s rights. Nowhere in the agreements is it addressed how the doctors can access records if needed. A patient’s life may literally hang in the balance before the practice can reach customer service and attempt to get information.

Another concerning issue is limiting liability. It may be typical to see a software vendor disclaim any liability even if the vendor is the one who caused the harm, but this has far-reaching consequences for the practitioner, and perhaps the patient. For example, if patient records are mixed through a programming error, the vendor would be held blameless. (This may not count in states where gross negligence cannot be contracted away, though even then legal action would have to be taken in order for the issue to be addressed). Even if liability is placed on the vendor, it is also common to limit liability to a small set of fees paid, usually around 6 months’ worth. If there is a breach of privacy, medical records are mixed, loss of access occurs, or anything causes huge regulatory impacts happens, it’s simply a case of *buyer beware*.

Let’s say a doctor loses access to a patient’s medical records. Practically speaking, that patient essentially loses access to those records. So, who owns them?

Most contracts would state that the doctors own them (or that the vendor does). Generally, the vendor owns the right to grant or deny access. This makes ownership a moot point, because if the doctor cannot access them to provide care, transfer the information to another provider, or to give the record to the patient (a patient right under HIPAA) then the records are essentially being held hostage, which is not permitted. Even HIPAA provides that a doctor cannot withhold medical records pending payment for care—but these vendors can, and do.⁵

There are some common scenarios which complicate this even further; eg, doctors may pass away, or retire or leave the practice of medicine without notice. In each of these scenarios, there would be a problem immediately accessing EHRs without some kind of arrangement already in place. The EHR vendors do accommodate authorized users, but what if there isn’t one?

If the only way to validate an authorized user is through the doctor, and that doctor is unavailable, then there will be issues getting patients the care they need in a timely fashion. And remember, the vendor has essentially no liability, per contract. In most cases, the vendors also state that they have no responsibility to accommodate patient rights directly, and it is common practice for a business associate (as defined under HIPAA) to defer patient access requests back to the provider.

Addressing these serious concerns will take either reasonable minds to work out common practice standards for EHRs or a tragic event where medical records are inaccessible, resulting in dire consequences.

It is not truly *ownership* that is the issue, so much as *control*. There are many interests here, all with valid legal considerations. Each professional must document findings; entities must document care and billing; associated vendors must document their actions; and patients need the information available. In the end, a legal, ultimate source record must be kept; the fundamental question is, who has the keys to it? It should not be the EHR vendor with ultimate control, and, despite their protestations to the contrary, the contracts give the EHR vendors critical access control.

What You Can Do

What can doctors do now, especially if they have little bargaining power? Read the contracts with the EHR vendors and negotiate using the law. *Doctors should carefully read the contracts anyway, given the incredibly broad authorization EHR vendors have to use the data in many ways. Selling to medical practices is not the EHR vendors’ only business model, by far; the data part is far more lucrative, in fact.*

If doctors cannot withhold records from patients for lack of payment, then there must be a mechanism to ensure records are not withheld from doctors. In the case of nonpayment, records are returned to the doctors in a readable format. If a doctor is no longer practicing (for whatever reason), the employer, estate trustee, and/or medical board are notified and a set of procedures would already be in place per state law. In such cases, records could not be deposited with the trustee as that would violate privacy laws; however, the trustee could be notified of available options.

The question for the EHR vendor is, if the physician is no longer practicing, who is responsible for maintaining the records for the legal retention time (which could be decades when minors are considered, as the retention clock generally starts ticking once patients reach adulthood)?

Further, interest groups, such as the American Medical Association, should issue clear guidance on this topic to acquaint practitioners with the legal issues and potential solutions. A set of industry standards that all EHR vendors (both direct and associated records with various vendors) must adhere to is recommended, even if this is a self-regulated effort. Medical records are too important to leave this issue unattended. ■

References

- Centers for Medicare and Medicaid Services. Electronic health records. Available at: <https://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html?redirect=/ehealthrecords>. Accessed January 20, 2017.
- NH Rev Stat Ann. §151:21.
- Health Information & the Law. Who owns medical records: 50 state comparison. Available at: <http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison>. Accessed January 20, 2017.
- Terry K. Patient records: the struggle for ownership. *Medical Economics*. December 10, 2015. Available at: <http://medicaleconomics.modernmedicine.com/medical-economics/news/patient-records-struggle-ownership>. Accessed January 20, 2017.
- U.S. Department of Health and Human Services. Health Information Privacy. Is a health care provider permitted to deny an individual’s request for access because the individual has not paid for health care services provided to the individual? Available at: <https://www.hhs.gov/hipaa/for-professionals/faq/2065/is-a-health-care-provider-permitted-to-deny/index.html>. Accessed January 20, 2017.