The First Wave

By Chad P. Brouillard

With new technology comes the potential for new risks and liabilities for your clients.

Emerging Trends in Electronic Health Record Liability

Given recent governmental incentives for medical practices and institutions to implement electronic health record software, much attention has focused on the efficiencies and technical advances of these new applications.

In 2009, the American Recovery and Reinvestment Act (ARRA), which included the Health Information Technology for Economic and Clinical Health Act, became law. The Health Information Technology for Economic and Clinical Health Act, also called the HITECH Act, appropriated nearly 20 billion stimulus dollars to encourage hospitals, doctors and other health care professionals to develop and implement electronic health record (EHR) systems. When health care practices install health care information technologies, sometimes they overlook the attendant risks of implementing, using and storing EHRs, which have developed fairly recently. Due to the newness of EHRs, we still do not completely understand the risks that they might bring. The first wave of legal consequences from such a fundamental shift in clinical documentation has begun to emerge. A host of new statutes and regulations, including the HITECH Act, now govern the functionality and substance of EHR systems, and the HITECH Act specifically enhances data security rules under HIPAA. Courts have started to consider legal matters of first impression involving EHRs, and our clients have become enmeshed in these cases with greater frequency.

As with most technological advances in the medical field, EHRs carry new forms of potential risk and liability. This article will sketch some basic areas of medical liability involving EHRs and will suggest ways that these risks may impact medical providers’ practices and, perhaps, the standards of care. Also, from the health care law and medical liability perspective, EHRs mark a fundamental shift in how we use and collect electronic medical evidence, as well as what we must think about when anticipating health care litigation.

My EHR Is Not the Same as Your EHR

When implementing any new health care process, we can expect some confusion and chaos. For one, generally, definitions initially will differ until the field comes to consensus about them. The term “electronic medical record,” for example, although technically distinct from an electronic health record (EHR), is commonly and confusingly used as a synonym for an EHR in the industry. For simplicity, this
The federal government seems to be creating demand for EHR systems that are certified or otherwise meet this minimum, “meaningful use,” functionality criteria. Implementing new health-care related information-technology processes, however, is complicated further due to the multiplicity of EHR vendor solutions available—over 200—and very little in the way of standards. For years, the EHR field had been the metaphorical Wild West, with few mandated guidelines about how a product functioned, communicated with other products, or secured its data. Certifying organizations, such as the Certification Commission for Healthcare Information Technology, endeavored to fill the gap by developing some minimum standards regarding functionality, security, and interoperability of EHR systems. Such efforts were limited—only applying if a software vendor sought to voluntarily seek certification or a purchaser required certification. Also, various health-care related information-technology organizations, such as the American Health Information Management Association, have tried to bridge the gap of best practices related to software implementation and use.

In February 2009, the ARRA mandated the development of “meaningful use” criteria to ensure minimal functional and security standards in EHR systems. For a health care provider to be eligible for stimulus funds, a provider will have to demonstrate “meaningful use” of an EHR system. The federal government seemed to be creating demand for EHR systems that are certified or otherwise meet this minimum, “meaningful use,” functionality criteria. On December 30, 2009, the first iteration of the “meaningful use” criteria was published, with further updates from the Center for Medicare and Medicaid Services to come. The “meaningful use” criteria outlined the technological objectives, features, and measures to gauge whether a particular EHR system qualified under the statute during Stage I implementation of the HITECH Act (2011). The current list includes objectives such as using computer provider order entry, drug-allergy checks, and e-prescribing, among many others.

The important point about these developing EHR functional standards is that health care and medical liability attorneys need to understand that an EHR system in one practice may not mean or do the same thing in another practice. Until you become familiar with the health-care information-technology used in your client’s practice, you can make few assumptions about how a product functions, communicates with other products, or secures protected medical data. For that reason, counsel for health care providers often find that in defending medical liability and health care cases involving data stored in an EHR system, it has become increasingly important to partner with clients’ information technology employees or consultants to clarify the technical issues and interoperability associated with the specific software involved.

Also, just because a medical office practice is small, it does not mean that the practice will employ an unsophisticated EHR system. Large institutions may share or even mandate the use of particular EHR software to best coordinate care among affiliated providers. A large institution likely chose EHR software that served its own clinical and economic needs. A small medical provider might have adopted a very sophisticated EHR application, possibly without having the same level of resources to deal with technical problems than you would expect in a large institution.

In any event, it is clear that given health care providers’ growing obligations related to the use and storage of medical information, choosing the wrong EHR software may create liability issues for our clients. Without technical, EHR-system guidelines that have been aligned to comply with health care regulations, e-discovery rules, and other laws, this liability will likely persist for years to come.

The Evolving Standards of Care for Clinical Documentation

The clinical world is in a state of massive transition centered on electronic documentation. It would be easy to underestimate this shift, to assume that it simply involves copying existing paper charting and “translating” it into a legible, electronic form. EHR software does not merely put printed progress notes onto a computer screen. It can store a person’s lifetime medical history in one central repository. With EHR software, a clinician can harvest a patient’s pertinent, clinical history from prior encounters with other health care providers and marshal them for present use. Critical lab data and vitals can trigger immediate alerts to a clinician in real time. EHR software automatically can flag contraindicated medications, preventing a clinician from even prescribing particular medicines. An office practice and medical center a hundred miles away from one another can instantly share up-to-date information on a mutual patient so that by the time the patient has traveled from the practice to the medical center, the medical center has the latest office visit record in the patient’s chart. Specialists from around the world can now use health care technology to collaborate on patient care, which previously might have been cost prohibitive. I cannot say enough about the potential, transformative benefits of this technology. More to the point, EHR is simply not a passive tablet on which to record medical data. EHR can actively coordinate the data drawn from clinical care.

What effect will health-care information-technology advances have on the standards of care for clinical documentation? An early Oklahoma state court case, Johnson v. Hillcrest Health Center, Inc., 70 P.3d 811 (Okla. 2003), pondered the same question seven years ago in a way that illuminates the present discussion. The case involved a motion for summary judgment brought by the defendant, a hospital, in a medical malpractice case. The basic claim was that the hospital’s employees had negligently failed to chart critical lab results in the paper clinical record. The twist in the case was that the information was reported
in the hospital’s electronic health record. Interestingly, the court in the Johnson case suggested that what the average reasonable person would conclude was the standard of care for clinical documentation practices may have shifted between 1997 and 2003 given the then increasing support and reliance on health-care information-technology in the medical field.

The health care industry has progressed much farther down the information-technology track in 2010. This is in large part due to the economic incentives in the stimulus funds and exemptions to the Stark Law, which governs Medicare and Medicaid physician self-referrals. State and federal mandates may increasingly prompt information technology reliance, as may economic penalties imposed on providers, scheduled to begin in 2015, for not meaningfully using EHR systems or other forms of health-care information-technologies. Once the mandate deadlines have come and gone, by the end of this decade, or if most health care providers and institutions have voluntarily adopted EHRs for clinical documentation, then failing to use the documentation technology could conceivably be offered as evidence of a deviation from the standards of care for clinical documentation.

It seems the standards of care for clinical documentation may have come full circle since the Johnson case. In 1997, an average person may have found that the standards of care for clinical documentation required documentation in a paper as opposed to electronic form. In 2003, the court in Johnson noted that due to the emerging use of EHRs the standard perhaps had shifted toward considering computer-based documentation as an equivalent substitute for paper charting. In 2010, given the advances in health-care information-technology and general reliance on it in the industry, we certainly are approaching the other end of the spectrum, where electronic documentation may be seen as most crucial.

Once we do reach that point, it seems logical that a liability inquiry will turn to how information technology has been used by clinicians and whether that use itself comports with the standard of care for maintaining and using medical records. Although actual case law may not exist on these nitty-gritty, technical-clinical issues at present, a great deal of ink has been spent on the risk management and health information management to describe the dangers of using templates, or copying and pasting information into an her system, providers sharing logins, providers modifying or deleting electronic entries after the fact of treatment, and other user-related issues. For the most part, juries may end up deciding what sorts of EHR practices constitute reasonable, clinical standards of care for clinical documentation.

The EHR as the Clinical “Source of Truth”

Health care institutions do not operate in an entirely paper or electronic existence. Inevitable paper processes still persist in every hospital system in the country. Most health care institutions employ a hybrid model in which both electronic and paper processes coexist. Making sure that health care providers query the correct electronic and paper sources to locate all necessary clinical information certainly is challenging. Unfortunately, health care institutions often have and maintain more than two concurrent sources of medical information. Both systemic and user-based challenges may prevent a clinician from accessing the relevant patient data when needed.

System Error

If choosing an EHR software from the hundreds of vendors, which may or may not comply with the various legal obligations placed on a provider, is itself a liability concern, then imagine a modern health care institution that maintains several EHR systems. For example, an Emergency Department may have a unique system, Labor & Delivery another, and Radiology yet another. Given the multiplicity of systems, it may take a great deal of technical effort to ensure that medical data in an electronic chart provides a uniform, “source of truth” about a patient that all practitioners can rely on in life or death medical situations. When technical means cannot centralize the information, the challenge then becomes training providers where to find particular information.

Human error only partially accounts for the inability to use an EHR system as a single source of truth. By design or due to implementation, an EHR system may not offer access to all possible data sources. Currently, it is not unheard of to find that one proprietary EHR system cannot share data with another in the same health care institution. Also, due to the low expense associated with data storage compared to the expenses associated with storing paper, the potential amount of information that a system could store about the medical life of one patient in one data source alone could become staggering. For example, in the current market, buying 1TB of storage space (1,000 GB) costs under $100. When multiple interoperable, EHR systems share data sources, the possible data volume multiplies. For a human user, contemplating manually searching this voluminous data becomes unimaginable. On the flip side, it is also a considerable technological task to create software solutions that can marshal all the relevant patient data from every data source that may pertain to any given clinical situation, especially when those clinical situations may not be contemplated a priori at the time of coding.

Another technical issue concerns the data integrity of stored information. Anyone who has used a database may have had experience with corrupted or misplaced information. For example, legal billing systems in a modern law office sometimes disrupt data due to database integrity issues. It is very possible for the same thing to happen to an EHR even with strict technical controls in place. The practical effect is that an EHR system may provide erroneous or incomplete information on a patient to a physician. As one author put it, “otherwise healthy patients are arriving at a provider’s offices to hear that they have diabetes, sleep apnea, or high blood pressure. When in actuality, doctors are reading the wrong records because master patient indexes were compromised.” AHIMA Advantage, EHR Anxiety? HIM Is What the Doctor Ordered, Apr. 2010.

User Error

A clinician can discover that keeping track of which data repository stores the correct pieces of medical data can be challenging. Are the lab results returned electronically or on paper? Do the results populate in one EHR or another? For this reason, liability cases now unsurprisingly may involve a clinician’s attempt to sort through data sources to find accurate clinical informa-
requesting his electronic health records. *Dominguez v. Wickremasinghe*, 2010 WL 625840 (Cal. St. App. 2010). From this case, we might infer that a patient’s constructive knowledge of the cause of his or her injury might begin once the relevant information had been recorded on paper or in an electronic health record. This obligation would also seem to put pressure on the plaintiffs’ bar to investigate electronic sources.

**The EHR as the Legal “Source of Truth”**

Defense counsel for health care practitioners and institutions also increasingly need clarity about the “truthful source” of a patient’s clinical encounter. To start, a defense attorney is usually not privy to the same EHR information in the same format as a client. When a client accesses an electronic health record, he or she typically accesses it through a graphical interface, often in dashboard or window form, which permits access to many sources of clinical information at the same time. Once a pleading has been filed, defense counsel often receives a print copy of the data contained in the EHR system in a word-processed format, which does not capture the look or feel of the interface that a clinician originally had available to him or her. Ask your clients and their in-house counsel if they can provide you with access to the interface that your clients use, even if only temporarily, so that you can have a feel for how the product that created the documentation looks and works. Be sure also to ask if any legal constraints prevent your doing so, such as contractual terms with the vendor or HIPAA provisions.

A print copy of an electronic medical chart also may lack metadata or audit trail information. Metadata is typically defined as data about data. It is data that indicates how and when a computer or application was used and by which login. Every software application may have its own customized metadata, which in health care can indicate when a user had access to medical information and what they did with it. Thus, if your case deals with when a medical entry was authored, when an entry was modified or deleted or when a lab report was accessed by your client, the story may involve more than an EHR’s printout indicates.

A final consideration for the health care litigator is which data sources the client searched to produce the record for you. Recalling the lessons from above, you may have a printout from one EHR system used in the facility but not another. Your client may not have provided an older, paper record kept in storage. Your client may not understand that you want the relevant data from all core data sources, not just the one that is the easiest from which to print that contains the bulk of the clinical information. A clinician may not technically understand which data sources contain evidence that would help you defend him or her.

Also, a health care litigator may have to think outside of the EHR box for data sources. Your client may have referred to pertinent emails between clinicians that were contained in the chart, but not provide those emails to you. Your client may use a smartphone to communicate with others and handle scheduling. Medical devices, such as vacuums in the labor and delivery unit, may contain chips that store basic information, such as when the device is turned on or off. All of these forms of electronic data can prove compelling objective evidence about the timing of events.

Since the widespread adoption of EHRs, fairly commonly medical malpractice defense counsel will receive several different versions of a legal health record from the same nonparty medical provider in response to routine subpoena requests. The reason is that different data custodians will pull records from different sources. To prevent missing useful electronic evidence, you often need to ask questions. Until you know the technological lay of the land at a particular institution, it is invaluable to speak frequently with your client’s in-house IT department or consultants if you can about which data is accessible and how.

**Work-Arounds and Subverting the System**

Another ground for liability may occur when clinicians intentionally or accidentally subvert information technology institutional protocols. We all understand work-arounds. Most often, well-intentioned clinicians intentionally override EHR system protocols making use of work-arounds. Clinicians can be very sophisticated users of health care technologies, having considerable technical skills, and they devise an infinite number of work-arounds in a good-
faith effort to introduce efficiencies into their departments.

This problem persists in the EHR environment in several ways, but essentially occurs when a clinician will directly or indirectly override a mandatory EHR protocol. These mandatory protocols may have been developed by someone who is not a clinician or does not work in a clinical department, and they may not reflect the “on the ground” realities of a clinical setting or particular departments. Clinicians may consider the protocols inefficient and burdensome. Prohibitive costs might make changing the protocols impossible. Clinicians then are left with an obstructing protocol that is a detriment in a fast-pace, demanding environment, which then leads them to create work-arounds to deal with the protocol’s problems.

One common way that a clinician may subvert an EHR system protocol involves clinical decision-making. Although it depends on the software, many systems can essentially issue an alert based on the entry of a certain clinical finding, result, or adverse drug interaction, which then prompts a user to make a clinical decision. Sometimes a system will even suggest a clinical course to a user. On its face, this prompt and alert system seems very useful. If the prompt or alert is based on incomplete clinical data, however, it may put a clinicians in a position in which he or she must override the suggested course or becomes distracted by routine, needless prompts. In many situations, if clinicians have the full picture, exercising professional judgment and overriding the suggested protocols may be clinically appropriate.

On the other hand, sometimes a well-intentioned work-around can lead to bad results. A recent matter involving a nurse in Wisconsin had lethal results for a patient when the nurse reportedly subverted the safety features of bar-scanning, medical-compliance software. The Joint Commission Journal on Quality and Patient Safety reported on the death of a 16-year-old pregnant mother who suffered a cardiovascular collapse when “an infusion intended exclusively for the epidural route was connected to the patient’s peripheral IV line and infused by pump.” Volume 36, No. 4, Apr. 2010. According to the journal, one of the root causes of the incident was that the nurse “did not place an identification band on the patient, which was required to utilize the bar-coding system to match the prescribed drug therapy with the selected/administered drug therapy” and “failed to use the available POC bar-coding system that could have detected the drug selection error before administration.” Some reasons why the nurse may have subverted the safety features included, among others, that the department nurses had collectively practiced deviating from the protocols, the department training on the software was suboptimal, the technology was recently implemented and often not fully functional for scanning IV bags and the protocols were perceived as not urgent in contrast to the normal patient demands in the labor and delivery unit. Ironically, the article describes the nurse as very caring, employing a patient-centric approach in her time with the patient and family, spending a good deal of time with them face-to-face as the unfortunate error occurred.

This matter was tragic for the patient and the nurse. It is also a sobering example of how implementing electronic health record protocols can create enormous potential liability for both an institution that installs a faulty protocol and the end-user, a clinician, who may employ a work-around to address an imperfect protocol.

Data Breach
One area of emerging liability comes from federal and state laws and regulations governing data breach of personal information. Protected data can include both protected health information as defined by HIPAA, but also other sorts of personal information, for instance, identifiers such as date of birth, residential address or social security numbers, or financial information, such as credit card numbers or bank account numbers. See HITECH Breach Notification Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009). Of course, most health care providers must follow the data breach procedures found in both HIPAA and ARRA and follow the Health and Human Services technical and procedural guidelines for reporting. In addition, a data breach may fall under the Federal Trade Commission’s Red Flag Rules (although currently an exemption for health care providers is being considered in the legislature.) See Identity Theft

Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, Final Rule, 72 Fed. Reg. 63,717 (Nov. 9, 2007). To further complicate matters, most states now have data breach rules that sometimes have reporting obligations that conflict with the federal requirements.

Liability does not end with data breach reporting. Under state and federal law, a consumer may sue a health provider if he or she is damaged by a data breach involving protected health information. Also, plaintiffs have employed traditional, common law theories, such as breach of contract and negligent infliction of emotional distress. See Yath v. Fairview Clinics, N. P., 767 N.W.2d 34 (Minn. Ct. App. 2009). A plaintiffs’ bar niche area is currently developing to bring these suits. See Regan-Touhy v. Walgreen Co., 526 F.3d 641 (10th Cir. 2008) (involving an electronic discovery dispute for a claim of wrongful electronic disclosure of private health information by a pharmacy employee).

Expansion of Direct, Vicarious or Third-Party Liability
Another area of potential expanded liability comes from medical institutions’ increased obligations when they install, maintain or connect to an electronic health records system and allow health providers and other institutions to have access to them. Obviously, the potential direct liability springs from the obligation to use reasonable care when installing and maintaining this software. If, for example, an EHR system is set up to import laboratory reports from another EHR system within the institution, and the software corrupts imported data leading to insufficient follow up on abnormal results, the institution could face potential, direct liability.

The very act of providing an integrated electronic health records system to clinicians may also increase vicarious liability for the acts of independent providers if they use the system, potentially raising third-party claims. In many states, physicians are not often directly employed by health care institutions but act as independent contractors with privileges to practice in institutions. Despite the contractual relationships, plaintiffs have argued that employment relationships exist under the common law between the institutions and
clinicians. See Restatement (Second) of Agency §220(2) (1958). Jurisdictions adopting the Restatement’s position employ multifactor tests to determine when an independent contractor can be considered an employee. Most germane to this discussion is whether providing an EHR system constitutes providing instrumentalities of the work or can constitute control over the mandated electronic database as a ground for expanding liability to third persons. Sanchez v. Wal-Mart, 221 P.3d 1276 (Nev. 2009). The case involved a woman who instigated a car accident while under the influence of prescription drugs, resulting in the death of another motorist and the injury of yet one other. The appellants sued a number of pharmacies that had filled multiple prescriptions for the motorist who caused the accident. Nevada has a statutory scheme requiring the pharmacies in question to participate in a computerized, prescription-tracking system designed to identify prescription drug abuse. While the appeal was unsuccessful for a number of reasons, one of which was that the pharmacies did not have direct access to the database, it does again raise the fundamental questions, if health providers add new data sources about patients to existing sources, does it create obligations to the patients or others, and if so, when? In Sanchez the issue was not so much the medical status of the initial tortfeasor, the woman who caused the accident, as it was her substance abuse, which was dangerous to third parties. If such information is made available to providers, plaintiffs may continue to claim that knowledge of a patient’s dangerousness creates special obligations.

Under state and federal law, a consumer may sue a health provider if he or she is damaged by a data breach involving protected health information.

details of a clinician’s work.

The courts have not offered guidance yet on the first topic, but on the second, a federal district court judge declined to find an employment relationship between the Department of Veterans Affairs and the United States of America and an independent contractor physicians’ group based, in part, on the physicians’ use of the Department of Veterans Affairs’ electronic health records system. Gibbons v. Fronton, 533 F. Supp. 2d 449 (2008). Although a success for these particular physicians, the plaintiff’s argument about the electronic health records system was limited because the software was used only to control follow-up tests, and the Department of Veterans Affairs maintained exclusive possession over the health records. From that point of view, the electronic health records system was not much different from paper records in terms of exclusivity of control. It is difficult to know what a court would do with a fully enabled EHR system with features such as “order entry” and clinical decision support making tools, software that interprets patient details to suggest treatment or interacts with clinicians as they exercise judgment.

Another interesting case tried to use a pharmacy’s participation in a state-

Electronic Discovery Exposure

In November 2007, DRI first published my article, “The Impact of E-Discovery in Health Care,” discussing the likely effect that e-discovery rules, as embodied in the then-new Federal Rules of Civil Procedure, would have on the health care industry, especially given the growing use of electronic health records. Without repeating the material covered in that article, since November 2007, e-discovery law as it applies to health care providers has developed further. In short, it is very clear that the e-discovery rules as embodied in the Federal Rules of Civil Procedure do apply to health care litigants.

Importantly, the rules have never contained an exception for the health care industry; they apply equally to all litigants. The case law has since demonstrated that the law will not treat health care institutions any differently than any other litigant when deciding e-discovery disputes. See Cason-Merenda v. Detroit Medical Center, No. 06-15601, 2008 WL 2714239 (E.D. Mich. 2008) (denying e-discovery cost-shifting motion on behalf of two health system subsidiaries in antitrust class action lawsuit resulting in burden placed solely on health system); see United Med. Supply Co. Inc. v. United States, No. 03-289C, 77 Fed. Cl. 257 (Fed. Cl. 2007) (sanctioning the government for failure to have medical treatment facilities preserve e-discovery); Regan-Touhy v. Walgreen Co., 526 F.3d 641 (10th Cir. 2008) (upholding the district court’s determination the e-discovery obligations met by provider, without producing audit trail for who had viewed electronic record as opposed to conducted transactions). The amended rules have been applied to parties regardless of industry or whether or not they are prepared for or have been accustomed to e-discovery. The rules have been applied to large businesses, small businesses, and even individuals. See Teague v. Target, No. 3:06CV191, WL 2007 1041191 (W.D.N.C. Apr. 4, 2007) (sanctioning an individual plaintiff with a spoliation charge for failure to preserve a laptop). Thus, health care institutions that basically have not prepared to respond to e-discovery requests remain increasingly vulnerable to both monetary and discovery sanctions over time.

Relative inexperience with e-discovery is not health care’s only problem. Many EHR systems, which generate an enormous amount of electronic data, were implemented before the e-discovery rules went into effect, probably without considering impending e-discovery obligations. As such, unlike many other industries, health care providers are probably uniquely exposed because they may lack the expertise and proper tools to meet the potentially immense discovery obligations that their revolutionary systems create. At present, health care institutions are still especially vulnerable to e-discovery requests due to failures to identify, locate, and produce all relevant data, failures to retain or store data, and failures to preserve data in its original form once a litigation hold has been issued, particularly in actively used or live EHR databases. It is relatively easy under federal law to accidentally spoil electronic evidence, therefore, a medical institution or practice that has never before

EHR Liability, continued on page 87
EHR Liability, from page 44
faced electronic evidence may need to routinely use technology consultants.

Conclusion
Although EHRs have now achieved mainstream, clinical adoption, EHR-related liability trends have not developed fully. At this early point, we can discern some potential liability areas. In an early EHR implementation stage, source of truth issues and expansion of liability issues may arise. In using EHR systems, the evolving standards of care for clinical documentation and work-arounds pose risks. Security as mandated by data breach laws or retention and storage issues involving e-discovery liability and data integrity have also emerged as important areas. Also, from a health care law and medical liability perspective, defense counsel must become extremely attuned to the conceptual and practical differences at play in most electronic health documentation systems. When in doubt, seek technical assistance from within or even outside an institution, otherwise you may miss a great deal of information to help your client’s case.