Pearls in a Sea of Uncertainty: A Primer on Potential Liabilities in Electronic Medical Records

Marie C. Moseley, BSN, CNNP, MPH, JD
University Health Systems of Eastern Carolina Inc.
Greenville, NC

In attempting to arrive at the truth, I have applied everywhere for information, but in scarcely an instance have I been able to obtain hospital records fit for any purpose of comparison. If they could be obtained…they would show subscribers how their money was being spent, what amount of good was really being done with it, or whether the money was not doing mischief rather than good….1

If you think the above quote was made by some healthcare provider dramatically lamenting the inefficiencies and inadequacies in the modern day medical record, think again. Although she was certainly a visionary in her time, Florence Nightingale would not likely have imagined that her words would still be ringing true more than 200 years after complaining about the then “modern” system of documenting a patient’s medical care.2 Today, more than seven years after the Institute of Medicine first identified health information technology as one of the “single most significant tools” that could help improve the quality of healthcare, the question is no longer of the “single most significant tools” that could help improve the quality of healthcare, the question is no longer of the “single most significant tools” that could help improve the quality of healthcare, the question is no longer of why EMRs are being implemented at record rates. Yet, despite their obvious significance, the unseen liabilities ingrained in EMRs have received little attention to date. This article is designed to help readers recognize some of the potential liabilities that exist throughout the lifecycle of an electronic records system, and to offer some pearls of wisdom in providing counsel on the issues identified.

e-Iatrogenesis

Iatrogenic: a Greek work defined as “induced inadvertently by a physician or surgeon or by medical treatment or diagnostic procedures.”4 You do not have to search long for the source of the term “e-Iatrogenesis,” a term recently coined by health information technology (HIT) professionals to describe the unintended patient harms caused by health information systems.5 Paper- and electronic-based medical records share in many of the same types of risks; e.g., harms resulting from data loss/destruction, inappropriate corrections, inaccurate entries, and unauthorized access. Over time, the EMR becomes a repository for voluminous amounts of data, plausibly resulting in a greater impact when the aforementioned risks are realized.

While hospitals are understandably reluctant to make public any unintended patient harms resulting from their own internal technology, some are willing. One hospital reported an increase in medication errors when implementing a computerized physician-order entry system (CPOE).6 Still another reported that it had actually seen an increase in mortality in its pediatric intensive care unit after implementing a CPOE system.7

As providers become more transparent in sharing their hard-earned lessons in implementing EMRs, e-iatrogenic harms should decrease. Counsel are encouraged to share their learned experiences by actively participating in EMR listserves.

• PEARL: Access a free searchable archive of relevant journal literature, maintained by PubMed Central, the U.S. National Institutes of Health, at www.pubmedcentral.nih.gov

Electronic Discovery

I am just saying, there’s nothing worse than a federal judge who thinks the discovery process is being screwed around with.8 If the admonition Judge Joseph M. Hood, U.S. District Court for the Eastern District of Kentucky, gave to defendants when ruling against them in an electronic discovery matter does not grab one’s attention, not much will. When the Federal Rules of Civil Procedure (Rules) were revised in 2006, new challenges to the discovery process were created. Under the revisions, electronically stored information (ESI) was specifically recognized as a distinct category of discoverable information.

The revisions laid out specific ground rules for what ESI is discoverable (mostly everything) and when it is discoverable (responsive party must be ready to identify all potentially relevant data within ninety-nine days of the filing),9 and attempted to provide clarification of the parties’ preservation and production obligations (duty to preserve ESI attaches when litigation can be “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it considers as “reasonably anticipated”). During the initial scheduling conference, the responsive party must also identify any ESI it plans on using in cross-claims or defense and/or what ESI it consid
are unaware of or inattentive to case law, legal developments, and regulations relating to electronically stored information—a critical shortcoming when the entity is faced with an electronic document discovery (EDD) matter. Failure to comply with the Rules carries significant risks not only for the hospital but also for its counsel. Significant sanctions may be imposed if the court determines that an abuse of discovery occurred or relevant ESI was destroyed in bad faith. Sanctions include adverse jury inferences, dismissal of claims/defenses, award of attorney’s fees and costs, and stiff monetary penalties. Under the Rules, the hospital’s counsel is equally responsible for compliance; hence, if discovery rules are violated, the lawyer may find him/herself sitting on the other side of the table—as the defendant in a legal malpractice case.

Some hospitals are under the belief that because medical malpractice cases are brought in state courts and hence not subject to the Rules (representing the majority of hospital cases), little, if any, resources need to be spent now in preparing for EDD, at least until their respective states adopt similar rules. While such an approach may seem reasonable, it ignores the fact that the hospital is subject to the Rules when before the federal court in at least two circumstances: (1) when a case is brought by the Equal Employment Opportunity Commission (EEOC); and (2) where complete diversity of jurisdiction exists in a medical malpractice case. For example, if a case is brought by the Equal Employment Opportunity Commission (EEOC), the hospital may find itself sitting on the other side of the table—as the defendant in a legal malpractice case. Failure to comply with the Rules carries significant risks not only for the hospital but also for its counsel. Significant sanctions may be imposed if the court determines that an abuse of discovery occurred or relevant ESI was destroyed in bad faith. Sanctions include adverse jury inferences, dismissal of claims/defenses, award of attorney’s fees and costs, and stiff monetary penalties. Under the Rules, the hospital’s counsel is equally responsible for compliance; hence, if discovery rules are violated, the lawyer may find him/herself sitting on the other side of the table—as the defendant in a legal malpractice case.

The importance of preparing the hospital for EDD cannot be overstated. Consider the enormity of just being able to identify the location of relevant ESI in a “typical” medical malpractice case: database files, word-processing files, PCs, laptops, desktops, PDAs, imaging systems, spreadsheets, discs, and backup tapes, to name a few—all of which are generated in multiple departments, are stored on different network servers, and that must be preserved from the moment litigation is reasonably anticipated. If the EMR supports a “mail box” function that permits users to email data from the EMR, the hospital must also determine what information was sent and to whom. Add that to the need to identify potentially relevant ESI existing in bio-medical equipment such as fetal heart monitors, blood pressure monitors, etc., and you begin to get a real sense of the complexity of e-discovery in the healthcare setting. Moreover, that does not even take into consideration the need to actually access, preserve, and produce it within the Rules strict deadlines.

- PEARL: Download and read a copy of the revised Rules with Committee Notes, available at www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.
- PEARL: Visit the following websites for publicly available e-discovery case databases, searchable by keyword:
- PEARL: Multidisciplinary response teams should be formed with representatives from Legal, Corporate Compliance, Information Technology (IT), Health Information Records Management (HIMS), Human Resources, Bio-Engineering, Finance, and Clinical Services. Each of the departments will play a critical role in the hospital’s ability to respond to a request for ESI in a consistent and efficient manner. When suitable, bring outside counsel to the table, as well as members of the executive team, who can assist the team in implementing its directives.
- PEARL: Designate two or more individuals who will serve as the hospital’s 30(b)(6) witnesses. The individuals should have institutional knowledge of what ESI exists, where it originates, and what its retention properties are. It will be counsel’s responsibility to make sure they also understand the legalities of collection, preservation, and production of the ESI.
- PEARL: Ask the hospital’s Chief Information Officer (CIO) to designate two or more individuals who will be primarily responsible for responding to EDD requests. Then, make sure they understand your “legal speak” and that you understand their “geek speak” before asking them to implement a litigation hold on ESI.

**Metadata**

By its very nature, the medical record serves as a valuable tool in proving—or defending against—an assertion of medical mal-
practice. Whether the paper record will best serve the plaintiff or defendant is largely dependent on two factors: (1) if the record accurately reflects the care that was provided to the patient; and (2) if it provides sufficient detail for the trier of fact to determine whether or not the standard of care was met in delivering the care. With electronic medical records, a third factor comes into play: that of metadata.

The easiest way to think about metadata is simply “data about data.” It is a sort of electronic “fingerprint” the computer generates whenever it manipulates an electronic document. For example, metadata will reveal what algorithms the system used in generating clinical alerts and warnings, and what their triggers were. In most instances it will also reveal what the user did in response to the warnings. For instance, if a provider overrides one of the system’s clinical alerts, metadata will not only reveal that the provider viewed the information, but also that he/she disregarded it.

Metadata also will reveal the who, what, and when of data creation, access, or modification. This is true even after the record has been “locked” from further data entry, so any later changes to the record must be clearly identified as an addendum. Failure to do so may be viewed as an inappropriate alteration of the record and can compromise its usefulness as a defense mechanism in litigation.

Metadata also serves a critical role in establishing the record’s reliability as admissible evidence, and it will be up to the attorney to convince the judge accordingly. As one judge so eloquently stated:

“I don’t care how much I try to understand meta-data, and residual data, and legacy data, and up data, and down data, and whatever…it is the lawyer’s responsibility not only to understand that and to know it, but also to be able to communicate it to me, so that I can make a decision if there is a dispute among the parties.”

Metadata can be particularly important in a medical malpractice case, especially when the substantive issue concerns if and when the defendant had access to some critical piece of information. The courts have not yet grappled with the question of whether or not the EMR creates a new standard of care, e.g., given the (presumed) ease in accessing all of the information available in the EMR, will a provider’s failure to review it constitute medical negligence? What about reliance on flawed clinical decision support mechanisms? Or a pattern of overriding clinically appropriate alerts?

Members of the plaintiff’s bar are becoming increasingly savvy about usefulness of metadata, and are now being advised to seek metadata whenever requesting medical records in discovery. Hospital counsel must be equally well versed and knowledgeable about what metadata exists in the EMR, what its functionality is, and what should be preserved in anticipation of litigation.


**Interoperability**

While a patient’s electronic health information may appear visually as a single record set when displayed on the screen, much of the data in the record may, in actuality, be generated by separate computer applications located throughout the hospital. Similar to building a paper record with documents generated from various departments within the hospital, an electronic record is built with data that is either pushed or pulled from other operating systems, oftentimes numbering in the hundreds. Each speaks its own computer language and may not be able to understand the meaning or context of data generated from another. By analogy, think about trying to run Windows-based software on a Mac system—it just does not compute. In order to build the EMR, there must be an “interface” solution that permits movement of the data between two or more operating systems with two or more databases.

Arguably, building an effective interface solution is the most critical factor in successfully implementing an EMR. Without reliable data exchange, the data in the EMR simply cannot be trusted. Unfortunately, it can take months, even years, for the software interface to be fully refined. Hence, it is crucial that the system be tested, tested, and retested. Premature or inadequate deployment of the EMR may give rise to allegations of corporate negligence.

- PEARL: It is important to fully test the system’s interoperability prior to going live. Failure to do so may result in inaccurate financial and/or clinical data, both of which can have significant negative impact on the hospital.

**Data Ownership**

As with any contract, limitations to the scope of potential liability may be addressed during contract negotiations; in fact, there are several good legal resources available that are specific to negotiating EMR agreements. Nevertheless, the issue of data ownership deserves mention.

The information gathered in an EMR system is a veritable goldmine for data miners. Oftentimes, the purchaser of the EMR does not consider the commercial value of the data as a ne-
negotiating tool when sitting at the table with the vendor. The right to disclose, sell, assign, and lease the data should remain with the hospital, and should be clearly stated in its license agreement. Should the hospital choose to permit vendor use of the data in any manner, it should be well compensated.

Unlike the hospital party in the agreement, the vendor is not considered a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and thus has little, if any, constraints in using the data. If the hospital is agreeable to designating the vendor as the owner of the data, it should have some say in how the vendor can or cannot use the data. At least one vendor has contracted to provide patient data detailing patients’ genetic information to a genetics research company for purposes of identifying genetic markers. Given the well-recognized concerns of discrimination by insurers and employers based on a person’s genetic predisposition, the sensitive nature of the data is of particular concern. Although the data will be disclosed in a “de-identified” format, it may nevertheless be possible to re-identify patients with relatively little effort.

Readers are cautioned to check applicable state laws before considering an agreement to grant the vendor any ownership rights, as even de-identified disclosures are actionable under some state laws.

Privacy and Security

The commitment to patient confidentiality exhibited by the healthcare community long precedes the myriad of federal and state laws that now govern the protection of patient confidentiality. This is not an easy feat, considering that roughly 150 people will have access to a patient’s record in a typical hospital stay, and that is in addition to the roughly 600 thousand payers, providers, and outside entities who have access for purposes of billing, utilization review, etc. Moreover, consider this: other than information technology, the only mechanisms available to the hospital in fulfilling its legal obligations are limited to policies, procedures, and protocols. Add the sheer volume of information collected in the EMR and implications of a security breach become staggering, and far exceed that which would result from breaching the confidentiality of a single paper record.

The hospital’s most prominent privacy obligations arise from the HIPAA Privacy Rule, which require the hospital, inter alia, to protect against reasonably anticipated threats to the security of electronic health information protected under the Act (ePHI); protect against reasonably anticipated inappropriate use or disclosure of ePHI; and assure its workforce complies with the Act’s Security Rule. There is no private cause of action under the regulations. Nevertheless, at least one appellate court has determined that a plaintiff may assert a violation of the Rules as the basis for a claim of negligence. In Acosta v Byrum, plaintiff asserted that her electronic medical records had been inappropriately accessed by an employee of a medical clinic, who then shared the information with a third party without her consent. Asserting that he had breached his duty owed under HIPAA and hospital policies, plaintiff named the clinic’s owner, alleging that he was negligent in sharing his password with the employee. The trial court dismissed for failure to state a claim upon which relief could be granted. The North Carolina Court of Appeals reversed, holding that while HIPAA does not create a private right of action, citing HIPAA may help establish breach of appropriate standards of care.

Electronic security breaches can be grouped into six categories, each of which present their own compliance challenges: (1) lost or misplaced records or hardware; (2) stolen records or hardware; (3) improper disposal; (4) unauthorized access; (5) unencrypted emails; and (6) unintended disclosure/release. Failure to implement adequate protections in any one category will result in vulnerabilities to potential data tampering, disruption of hospital operations, and inappropriate disclosure of sensitive information. However, the degree of protection that can/should be afforded to each category is limited, primarily by the security functions of the EMR itself, the proficiency of the IT staff, the commitment of hospital executives, and budgetary restrictions.

The impact of a security breach is multifaceted. Not only could the hospital be subject to a criminal penalty under federal and/or state law, but to civil damages, loss of community confidence (loss of revenue), and negative impact on employee morale as well (staff turnover → shortage of care providers → decreased patient satisfaction → loss of revenue). Additionally, the monetary expenditures necessary to offer credit monitoring services to affected individuals can reach upwards of millions of dollars. Such was the experience of the Department of Veterans Affairs (VA) last year when it reserved more than $20 million after discovering an external hard drive was missing from its Birmingham, AL, research facility. The hard drive contained sensitive information on an estimated 650,000 physicians and 254,000 veterans who were provided with credit monitoring services. What was the total cost per person? A mere $22.22 per person, on average.

Security breaches may also result in class action lawsuits as was brought against Providence Health Systems, when computer back-up tapes and disks containing patient information were stolen from the car of an employee who had taken them home to make back-ups. When Providence refused the patients’ request to offer credit monitoring services, they filed suit under theories of negligence, negligence per se, and unlawful trade. Providence eventually offered the credit services and the case was dismissed, just in time to reach a settlement agreement with the Oregon Department of Justice, which investigated the hospital following the theft.

A similar breach just unfolding at the University of Miami (UM) also bears watching. There, computer back-up tapes containing patient health information and other sensitive information were stolen from a vehicle belonging to its off-site storage company. The scope of the breach was huge: anyone who had been a patient of a UM physician or visited a UM facility at any time since January 1, 1999, was affected. UM anticipates it will provide notice to the approximate 47,000 patients whose financial information may have been compromised, but no public mention of offering credit monitoring services has been made.

- PEARL: Review the Government Accountability Office’s report to Congress, Lessons Learned About Data Breach Notification
Teaching Hospitals & Academic Medical Centers

8 Yong Y. Han, et al., Florence Nightingale, record that "shows what amount of good it can really do." A hand in achieving Florence Nightingale's vision of a medical technology. If adequately prepared, perhaps everyone will must become comfortable with multiple aspects of information health benefit information or health data (no mention of how the state plans to address jurisdictional issues raised). Whether other states will follow suit remains to be seen.

• PEARL: Stay abreast of your state's breach notification laws. Under sweeping revisions to California's data breach notification laws (effective January 2, 2008), any compromise to a resident's medical or health information is now subject to the state's data breach notification laws. Further, the law now applies to any business holding covered information, which would include any business with computerized employee health benefit information or health data (no mention of how the state plans to address jurisdictional issues raised). Whether other states will follow suit remains to be seen.

• PEARL: Educate, educate, educate. Make it painfully clear to users that even a seemingly simple thing like sharing log-on information could result in an erroneous audit trail that may someday be used against them. Give examples, such as leaving an active record open and failing to log out. In the event of someone else continuing the session without logging on themselves, the audit would appear as though the entire session was that of the original user, and this is problematic if the person who follows behind inappropriately peruses through other patient records.

Conclusion

What the ultimate liabilities in electronic medical records will be is unknown at this early stage of development. To assist the hospital in navigating its way through the uncertainties, counsel must become comfortable with multiple aspects of information technology. If adequately prepared, perhaps everyone will have a hand in achieving Florence Nightingale's vision of a medical record that "shows what amount of good it can really do."

1 Florence Nightingale, Notes on Hospitals, LONGMAN, GREEN and COMPANY 176 (1863).
6 Amy L. Potts, et al., Computerized Physician Order Entry and Medication Errors in a Pediatric Critical Care Unit, 113 PEDIATRICS 59-63 (Jan. 2004).
9 Rule 16(b) requires that the parties engage in a "meet and confer" conference within ninety-nine days of the case filing.
10 In the Matter of Michele Estrada, 143 P3d 731, 740 (N.M. 2006).
12 Some states have already revised their rules of civil procedure to mirror the Federal Rules. See Arizona 16 A.R.S. Rules of Civil Procedure. Rules 16(b), 16(c), 16(d), 26(a), 26.1, 26.2, 33(c), 34, 37(g), and 45 (Supp. 2008).
15 See Michael M. Vugoda and David A. Lubarsky, Failure to Recognize Loss of Incoming Data in an Anesthesiologist Record-Keeping System May Have Increased Medical Liability, 102 ANESTHESIA & ANALGESIA 1798-1802 (2006).
16 The Sedona Conference is a nonprofit, 501(c)(3), research, and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. Judges will often rely on deliverables created by its Working Groups (comprised of leading jurists, lawyers, experts, and consultants) when addressing issues involving electronic discovery. United States v. O'Kafe, 537 F. Supp. 2d 14 (D.D.C. 2006) (requiring defendant to preserve electronically stored information in its native form with metadata).
17 In litigation, public and private corporations, associations, and government entities speak through their designated representatives. Rule 30(b)(6) in both federal and state court Rules of Civil Procedure allow a party to request the deposition of a single individual representing an entity, whether a party or a non-party to the litigation. A 30(b)(6) witness is the individual designated by the responsive party as the person most knowledgeable about the subject of the deposition testimony.
23 On May 21, 2008, President George Bush signed into law the Genetic Information Nondiscrimination Act, Pub. L. No. 110-233, which prohibits insurers from seeking or using genetic information in a discriminatory manner.
29 Gibson v. Providence Health Sys.-Or., No. 0601-01059 (Multnomah County Cir. Ct., Or. 2005).
31 Announcement from the University of Miami, available at www.dataincident.miami.edu (last accessed Apr. 25, 2008).