

Special Edition on the Electronic Health Record



A VIEW FROM THE TRENCHES: DISCOVERY ISSUES WITH ELECTRONIC MEDICAL RECORDS

Matthew P. Keris, Esq.

Until about five years ago, if I asked a client to preserve & copy a patient's original medical record, it would be as simple as going to the file room, pulling the manila folder off the shelf, and having a file clerk copy each document completely, and then putting the original chart into a "legal lockdown" area, where access would be restricted to just a few individuals. But if I were to make this request now, it may not be as simple to produce and preserve the patient's information.

This change was brought about by two events, ironically arising at nearly at the same time: President Bush's call for the end of paper medical records through the adoption of a comprehensive, intertwined network of electronic recordkeeping by the midpoint of this decade, and; amendments to the Federal Rules of Civil Procedure that mandated the preservation, production and discovery of electronic data in addition to the paper record. These changes acknowledged the reality of the times--that almost all hard copy documents were generated by computer.

At the time, little did most anticipate how these developments would alter how medical professional liability claims are raised, investigated and defended. In conjunction with the push for electronic record keeping, portability of health information is encouraged via off-site networked computers, smartphones and laptops. On top of this, the new legal rules mandate that the parties and their counsel find and preserve relevant information in some instances before a lawsuit is even

filed. If this weren't enough, embedded "information about information" that did not exist with traditional medical records now can be considered relevant and discoverable, and must be maintained on an ongoing basis.

Approximately five years into the transition to electronic medical records, we are entering a time of great uncertainty because of the lack of legal and practical precedent on litigation discovery issues. Despite the lack of legal guidance, by knowing the potential hazards pertaining to electronic medical records, health care providers can significantly mitigate their expenses and limit their liability exposure. The following is an overview of the biggest changes and challenges that health care providers need to be aware of in the age of e-discovery.

FROM PHOTO ALBUM TO FACEBOOK: THE MEDICAL RECORD CAN BE ANYWHERE

Until recently, if people wanted to share childhood photos with others, it would require pulling out the photo album. Access to these photos was limited to whoever pulled the album out of the closet. Now, with the advent of Facebook and other social media internet sites, photographs are posted & emailed with little limitation as to who can view, save and share the pictures. Likewise, the medical record has also transformed itself from a safe, invite-only medium to a fluid, ever-evolving information vehicle that may never look the same way twice.

With electronic medical records, health information can be utilized in any combination of text, graphics or other information in digital form, created, maintained, modified, retrieved or distributed by computer. If they contain patient health information, emails, digital voicemails, computer

calendaring programs and wireless text messages may now be considered a part of a health record. Further, the proliferation of smartphones, laptops and computer smart-pads also increases the scope of where and how information may be reviewed and maintained. Management of text messaging is an example of where health care providers can run afoul of the new legal responsibilities in the management and production of relevant information.

If a patient passed a handwritten note containing health information to her physician, there is little doubt that this note would be considered relevant if a medical malpractice lawsuit was filed. Likewise, if the physician wrote a note to her patient as to what to do, it would also be relevant and discoverable. Is text-messaging anything different from passing handwritten notes? If a physician receives via text messaging health-related information pertaining to a patient for the purposes of treatment, there can be little debate whether this text would be considered a part of the medical record in a malpractice case. So I ask, how many of you preserve text messages, or incorporate them into the chart? Perhaps the better question is, *how many of you know how to preserve a text* (I don't!). My feeling is that few, if any, health care professionals are doing anything to preserve their text messages and this is not a good thing. Just as if portions of the hard copy record were destroyed or lost, the loss of relevant text messages can be detrimental to a health care provider in subsequent litigation. This is just one example of the issues health professionals and attorneys are facing in the age of electronic medical records and e-discovery.

So now, when I ask a client for a patient's record, it is easy to see that the search for the patient's record is no longer limited to the medical records department. The "medical record" is no longer pen & paper. Now, it is digitized and can be anywhere

and everywhere at the same time.

METADATA CHANGES DOCUMENTATION, ARCHIVING AND PRESERVATION OF DATA

The Federal Rules of Civil Procedure were amended to mandate that all parties and their attorneys, who are in or anticipate litigation, do everything in their power to preserve electronic data. As such, in every federal civil case, the parties must address with one another whether there is a technical issue pertaining to the preservation and production of electronic data (Rules 16 & 26). Further, when interrogatories (written questions) or request for production of documents are served, the parties are mandated to not only review the hard-copy record, but also the electronic record when drafting their responses (Rules 33 & 34). The Federal Rules also allow that the information requested be provided in native form (Rules 34 & 35), which can be a challenge. Lastly, in instances where electronic data was destroyed by honest mistake, a party may request a "safe harbor" excuse to their ongoing duty to preserve and produce electronic evidence and avoid sanction (Rule 37). These rules are applicable to all civil cases filed in the federal system and are not solely limited to medical malpractice claims.

From old emails to outdated spreadsheets, when a party anticipates litigation (medical malpractice or otherwise), they must cease routine data destruction and immediately institute data preservation practices, from the top to the bottom of an organization. If electronic data is destroyed at a time when litigation is ongoing or anticipated, it can result in extreme legal consequences, including contempt, spoliation and sanctions. Apart from court-ordered penalties, juries have punished parties who engage in lax data preservation practices in the form of exorbitant compensatory verdicts or the imposition of punitive damages.

From a legal evidentiary standpoint, nothing is better than "metadata" if there is a question as to the veracity of information placed in a record, whether it be in a letter, spreadsheet, email or electronic medical record. "Metadata" is the unseen, embedded "data about data" that tracks every keystroke to a computer. Because of metadata, delete does not mean "good-bye" and alterations and after-the-fact entries are 100% clear if someone wants to challenge the record. When the date, time, entry or source of entry is in dispute, metadata gives the "who, what, when & where" for everything.

In the context of a medical malpractice case, metadata will play a role if the timing of entries is relevant. It can reveal significant gaps in time if, for example, an entry for 10:00 am was electronically recorded at 2:30 pm, which could be at the end of a hospital nurse's shift. Using this example, nurses can be asked why there is a four-and-a-half hour time gap between the noted and actual entries. They can also be asked whether the entry is completely accurate as to what occurred or was observed at 10:00 am, or if the information recorded at 2:30 pm is less than accurate, based on the patient's change of condition during the four-and-a-half hour window. Most significantly, metadata will reveal with clarity if the record has been altered in any way once there is a negative patient outcome. More often than you care to know, health care providers are tempted to change a record to their benefit if they find out that they are being sued, or that a lawyer has requested a copy of the chart. With electronic medical records, there is no way to hide changes to the record, whether innocent or not.

In my opinion, metadata and the need to preserve it along with other electronically saved information, poses the biggest difference between the hard copy and electronic medical record. Those who fail to acknowledge its importance can place their legal

positions in significant jeopardy.

THE AVOIDANCE OF "GARBAGE IN, GARBAGE OUT" BY PROPER ELECTRONIC MEDICAL RECORD TRAINING & DOCUMENTATION

With every upgrade to an electronic medical record system, updated training will be required and it is essential that all users of the system be equally familiar with how information should be documented. If electronic medical record users do not know how to use, document or save information correctly, there will be charting errors that can increase treatment costs and obviously, increase the risk of a malpractice suit. Corrections to the record can also be difficult: if the electronic medical record system does not allow for consistent and uniform methods for corrections, it can also confuse the user and allow inaccuracies to snowball, resulting in inadequate care. Because each electronic medical record system is different and will be upgraded on a regular basis, training on system use, especially in correction-making, will be more frequent and vital.

Overreliance on one person ("power users") to show the other staff "how you do things" should also be avoided. This is especially true when a "power user" leaves for some reason. Documentation as a whole can suffer and it could become expensive in the absence of a "power user" because re-training of the entire group may be needed. The goal is to have everyone be a "power user."

The use of log-ins and log-offs will replace the traditional handwritten signature or initials adjacent to specific chart entries. The log-in has become the signature, and it should be stressed to the medical staff that entries under another's log-in will not be tolerated because it will not reflect an accurate record, for there is no other way to verify a persons'

e-charting in the absence of handwriting.

Lastly electronic medical record systems largely rely on the documentation of pertinent negatives ("charting by exception") which does not encourage detailed information and tempts users to "left click away" rather than use free-text narratives. If you are affiliated with more "senior" health care providers who are not comfortable typing, this may lead to an over-reliance on clicking, rather than the use of narratives, which can result in a dearth of valuable recorded information. Because of the reliance on "charting by exception" the use of the free-text narratives may be more important than ever and should constantly be encouraged. One warning, however, with respect to "free-text narratives"-the "copy/paste" function. Copying and pasting has its place, but its use should be the exception, rather than the rule. A user may be copying/pasting information in the chart that is inconsistent with the record, or just plain wrong.

WHAT A PRODUCTION!: EMR SYSTEMS NOT DESIGNED WITH LITIGATION IN MIND

One of the universal tenets of medical malpractice law is that health care providers will be held to the standard of care at the time at issue, rather than current standards. What is the standard at one time, may no longer be the standard at a later date due to medical advancements. What should have been done at the time at issue, not in the present, therefore, is the criterion that juries are instructed to utilize when evaluating standards of care. In this respect, old-fashioned hard copy records remain far superior to electronic medical records because they provide a static snapshot of how the record looked on the day at issue.

Electronic medical records systems were not designed to maintain a snapshot. Health information

now is recorded in electronic code, not ink, to ensure its fluidity, transferability and manipulation. And despite billions of dollars spent in system upgrades, it remains either impossible or cost-prohibitive to produce an entire paper copy of how a patient's record appeared on a computer monitor. What we are left with is a paper record that looks nothing like what is on the screen. The paper record can be confusing and appear unorganized compared to how it looked on the screen. This is very problematic for malpractice defense attorneys in several respects.

The main problem deals with depositions. The level of scrutiny of health care providers in a deposition setting can be overwhelming. Because of this, it is important for witnesses to have some level of comfort. However, when the printed record they are relying upon to provide their answers looks nothing like what is on the monitor, it can only add to a deponent's anxiety because of their unfamiliarity of the format. It may also result in inaccurate or incomplete answers. To rectify this situation, an attorney may consider bringing in a computer monitor to deposition so the witness can refer to the record as it would appear to them in practice. However, this decision is fraught with peril as well.

Electronic record systems are constantly being updated. The first version of an electronic medical record system may be in effect on the date at issue. Version two of an electronic medical records system may be in effect when the lawsuit is filed. By the time depositions are held, there can be a fourth version in place. With technical advancements in the electronic medical record, it may be impossible to replicate exactly how a record looked on a monitor, just as it is impossible to replicate how it looked on the date at issue on paper. Unless the health care provider has a means of showing how the record looked like on the monitor with version

Risk R_x

one several years after version one was obsolete, there may be no way to replicate how the screen appeared on the date at issue years later.

Another troubling issue is that if you utilize an electronic medical record as it appears on a monitor during a deposition, you may be educating your adversary of things the system can and cannot do. For example, by using a monitor during a deposition, it may reveal that certain health data can be leveraged for the purposes of providing automated treatment options. If the plaintiffs' lawyer learns this in a deposition, he may inquire if the leveraging function was utilized, and if not, why?

If you still are considering the use of a computer monitor during a deposition, yet another consideration is to bring in someone from information technology or medical records to the deposition to educate and assist the parties and witnesses as to what functions were available in the electronic medical record during the time at issue. By doing this, it will ensure that correct testimony is being provided as to system capability. However, it may mean that this person will be deposed individually as well.

There is no right or wrong answer in deciding whether to rely purely on a paper copy of an electronic medical record system for deposition, or to provide the opportunity for the witness to use the record as it appeared on the monitor. You may be left with deciding which is the lesser of two evils. These decisions should be made on a case-by-case basis, depending on a multitude of factors.

WILL YOUR ELECTRONIC MEDICAL RECORD VENDOR BE A PART OF THE PROBLEM OR THE SOLUTION?

For better or worse, your electronic medical record

vendor is similar to your spouse. In this period of transition, both health care providers and their vendors will face new ground that can test their relationship.

In jurisdictions that recognize a right for patients to recover under "corporate negligence," plaintiff lawyers may argue that health care suffered due to the selection and use of a deficient electronic medical record system. In other words, the officers of the institution are alleged to have committed systemic negligence, independent from the acts of its agent health care providers, by failing to have a proper and safe electronic medical record system. It can be argued that the system has gaps that precludes adequate record keeping; a system that encourages less-than-truthful entries by allowing "copy & paste" functions, or; the electronic medical record vendor failed to provide adequate training and education to the users. If a medical institution faces these allegations, consideration should be made to bring the electronic medical record vendor into the fold. What needs to be determined is if the vendor will be a part of the problem or a part of the solution. As a part of the solution, the vendor can provide their technical support and potential witnesses to blunt criticisms regarding their product. However, in some instances, consideration should be made to join the vendor as a party in the litigation for purposes of having them contribute to any settlement or verdict, or for indemnification purposes, in the event there is a judgment against the institution. This decision should not be taken lightly, because like a marriage, it can continue the relationship or lead to a divorce.

Another area where cooperation is needed with the vendor is if the plaintiff's lawyer requests patient health information in native form in accordance with Rules 34 & 35. In situations where plaintiffs seek native word processing, spreadsheet or email data, this request would not raise much concern.

This information can easily be viewed by plaintiffs' lawyers from their laptop using an off-the-shelf product that they can purchase. However, a plaintiff's lawyer cannot purchase an electronic medical record system from his neighborhood business chain superstore. In order for plaintiffs' lawyers to receive the native data and view it in their office is by providing either a copy of or access to the electronic medical record system. Neither of these options is desirable, for the reasons I outlined above (metadata; system limitations) but under the Federal Rules, it may be ordered and become necessary.

This is another situation where you again need to ask if the vendor is going to be a friend or foe. To utilize the electronic medical record vendor as a friend, you may ask them to intervene as a non-party and argue that plaintiffs' counsel should not be entitled to a copy of or access to the record in native form because of the possibility that they, after becoming familiar with the product, will share its "trade secrets" with rival vendors. Intervention by the vendor as another party objecting to the request to view the health information in native form also would be helpful in that it would automatically lend credibility to the objections and demonstrate that the issue is not another attempt by defense lawyers to "hide the truth."

RECOMMENDATIONS WHEN MEDICAL PROFESSIONAL LIABILITY CLAIM IS ANTICIPATED OR RAISED

Taking what we have learned from the changes to the law and the medical record, risk management protocols should reflect the following when a professional liability claim is anticipated or filed.

1. Initiate "litigation hold" process from top to bottom.

Once a claim is anticipated, the Federal Rules and precedent clearly mandate that both the parties and the attorney immediately institute a "litigation hold" or cessation of all electronic data destruction practices. A memo from management to staff, or an attorney stating "stop your data destruction" is not enough. The duty is quite stringent, and all necessary persons must be made aware of the litigation hold request by any means necessary, which remains ongoing through the litigation.

2. In addition to meeting with the client or risk manager, the attorney must meet with the "computer guys."

Under the Rules, a party's attorney must become familiar with his clients' document retention policies and computing infrastructure. Counsel for the party to the litigation must also know if there are any issues with the computing infrastructure that has limited the ability to archive and produce relevant information, including electronic data. If there are production issues, because data has been lost by honest mistake or routine protocol, it may be wise to reveal this early on so as to avoid spoliation or "cover up" allegations. Therefore, it is incumbent for counsel not only to learn about the care provided in a case, but also how the record of the care is maintained and produced.

You also want to meet with the "computer guys" to assess which one (if any) you would want to produce for a deposition on the electronic medical records system. What you are looking for is someone who is knowledgeable of the system, but at the same time, can think and answer questions adequately under pressure. Unfortunately, you may not have the ideal person in this regard, but on the other hand, you need to know who you absolutely cannot produce for fear of answering questions in a manner that would hurt your case.

3. Determine the production format.

In most cases, a paper copy of the electronic record should suffice. However, if the record is in question, there may be an attempt to obtain or view the data in native form, or have an e-discovery vendor search the system for documentation irregularities. If there is a push for the production of the data in native form, consider calling the vendor because they may not want a version of their product produced or in the hands of someone who would share it with a rival vendor.

4. Start gathering all your information on the electronic medical record system.

If you haven't already received written discovery requests pertaining to your electronic medical record system, be prepared: they will be coming. Requests for all types of documents should be anticipated, including contracts; training manuals; product information; confirmation of staff training, and; administrative documents surrounding the purchase of the electronic medical record system. Policies and procedures will also be requested regarding documentation standards; login & password use, and; correction standards for purposes of determining whether health care providers were in compliance with the same.

5. Educate deponents not only on the medicine, but also on any documentation issues.

Through thorough written discovery, plaintiffs' lawyers may glean a good working knowledge of the electronic medical record system; how it is to be used, and; pitfalls in the system. As such, in addition to the medicine, deponents should be made aware during deposition preparation if there are time gaps in documentation that was revealed

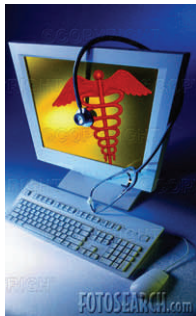
from the metadata; limitations and use of the electronic medical records system at the time at issue versus the present, and; policies & procedures from the time at issue with respect to data administration.

CLOSING THOUGHTS

In the haste of progress, issues that once seemed trivial can take a life on their own leaving the question, "was this such a good idea?" Many in health care risk management who are currently dealing with new discovery issues during the transition from hard copy charting to the adoption of an electronic medical record system may be asking if it was a wise decision to change. Documentation, production and preservation of the electronic medical record is ripe with professional liability pitfalls we failed to consider as recently as five years ago. Although we may desire a return to simpler times, make no mistake, there is no going back. The electronic medical record is here to stay and in medical professional liability litigation, as it was in the past with the hard copy chart, it can be your best friend or your worst enemy. The need for timely, complete and truthful charting remains static, but the impact in failing to abide by these principles is much greater with significant consequences. Instead of lamenting the decision to convert to an electronic medical record system, the better path is to embrace these changes. Those who won't will be doomed by applying 20th Century practices to a 21st Century world.

Matthew P. Keris, Esquire is a shareholder in the Scranton, PA office of Marshall, Dennehey, Warner, Coleman & Goggin where he extensively handles medical malpractice defense claims, representing physicians, professional groups, hospitals and regional health centers. He lectures extensively on issues pertaining to medical malpractice and is recognized nationally for his expertise in electronic medical record issues, having spoken to numerous organizations including American Society for Health Risk Management; American College of Obste-

trician/Gynecologists; the Pennsylvania Osteopathic Medical Association; The Commonwealth Medical College; Commonwealth of Pennsylvania MCARE Fund; Central Pennsylvania Association of Health Care Risk Management; Center for Health Training, and; PANPHA and for publications including National Health Law Week; Hospital Litigation Reporter and New York Health Law Update. He also advises medical institutions on the establishment of policies & procedures regarding responses to electronic discovery.



The Electronic Health Record: Keeping the Illegible From Becoming the Illogical

Joseph J. Tepas, III, M.D.
Professor Surgery and Pediatrics
University of Florida-Jacksonville
Campus

In November 1999, the Institute of Medicine released "To Err is Human" in which it reported that approximately 98,000 unexpected deaths occur every year in American hospitals. The fact that these patients were dying unnecessarily in the very places designed to preserve life is the core of the national mandate for a safer system of health care delivery. The report identifies, as a major system deficiency, the innumerable barriers to accurate and timely information exchange among members of the health care delivery system. One of the first recommendations for correcting this problem was the rapid implementation of electronic medical records as an alternative to dealing with illegible scrawl on prescriptions and in health records.

Shortly thereafter, many informatics companies began to market their versions of electronic medical health records, almost all of which today produce unstructured textual representations of what used to be written on a piece of paper tenuously attached to a notebook at the patient's bedside. As

the transformation of our health care system progresses, this tsunami of unstructured textual data will gradually evolve to a more specific structured format that will precisely define system performance and track clinical outcomes. Most importantly, this data will become the substrate for accurate clinical decision support. Until then, there are a number of factors regarding the emerging application of electronic health records that directly relate to the current daily practice of medicine. As always, these factors present both risks and rewards.

The rewards are fairly obvious. The display of information on a screen in front of the physician rather than on a piece of paper in no way implies better or more efficient health care. However, the fact that an electronic system contains all of the records that heretofore the physician had to dig out of endless paper files does provide immediate benefit. This, in concert with concurrent display of ancillary information, should facilitate the process of clinical care. Ultimately, accumulated data from numerous health records will emerge as an evidence base that will stimulate a more precise level of disease management and improve the overall quality and efficiency of health care.

The risks may be less apparent, but are no less real. The intent of electronic health records is to make information more accessible, accurate, and available, however, each presents significant potential for system or individual error.

Access:

The continued evolution of informatics technology now makes it possible to track information from practically anything with a circuit board and electric power source. Every one of these devices represents a potential breach in the security that should surround virtually every piece of data re-