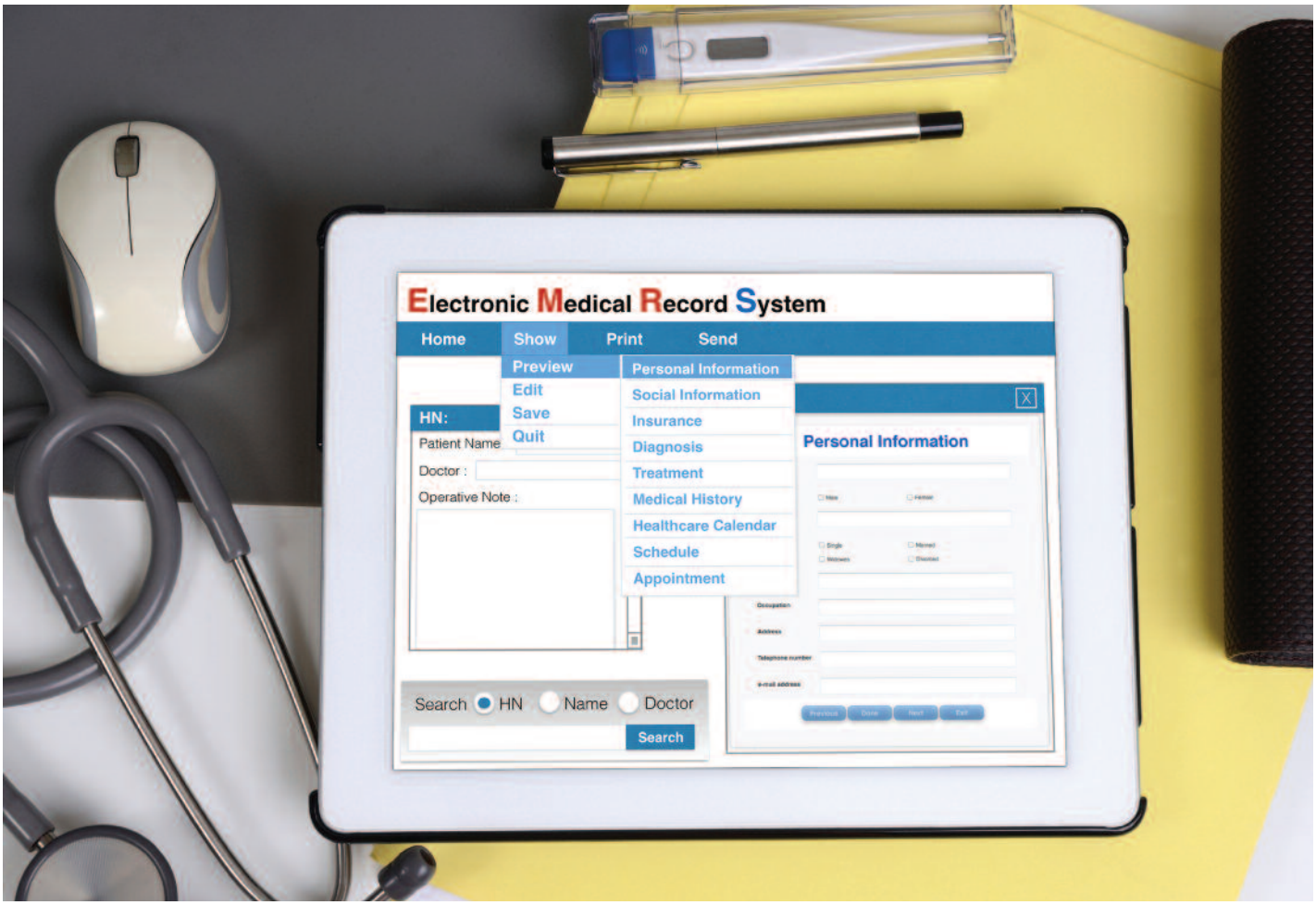

Electronic Medical Records

Changing Medical Malpractice Litigation

by Jonathan H. Lomurro

"By computerizing health records, we can avoid dangerous medical mistakes, reduce costs, and improve care." – President George W. Bush, State of the Union Address (Jan. 20, 2004)

"We will make sure that every doctor's office and hospital in this country is using cutting-edge technology and electronic medical records so that we can cut red tape, prevent medical mistakes, and help save billions of dollars each year." – President Barack H. Obama, Radio Address (Dec. 6, 2008)

Something both major political parties agreed upon has led to disagreement in the field of medical malpractice. While the contentious discussions on mandatory competence in technology for lawyers echo in our ears, technological advances have taken place in the field of medical malpractice and, as a result, practitioners are being forced to deal with these advancements. A lawyer's ability to adapt and accept will define his or her success; in litigation, ignorance is not bliss.

When the Health Information Technology for Economic and Clinical Health Act (HITECH), within the larger American

Recovery and Reinvestment Act of 2009 (ARRA), and the Patient Protection and Affordable Care Act (PPACA) were placed into effect, the field of medical malpractice was destined to change. With the change, the scope of discovery in medical malpractice vastly expanded. The reason for the expansion was HITECH's established goal for "utilization of a certified electronic health record [EHR] for each person in the United States by 2014."[1] In order to accomplish its goal, the government provided an electronic health records (EHR) incentive program for clinicians and hospitals that demonstrated meaningful use of electronic health records. With incentives and penalties driving conversion, almost all hospitals and most private practitioners have switched their practices over to electronically stored health records.

Foreseeing the risks associated with such a fast implementation of EHR in the country and a need for protection of these new electronic records, the Department of Health and Human Services (HHS) promulgated the privacy and security rules under the Health Insurance Portability and Accountability Act (HIPPA).[2] The rules created standards to address how health information may be used and protected. One of its purposes was to ensure that medical records could not be altered without detection; "protect the security and privacy of individual identifiable health information (IIHI)."[3]

The HIPAA security rule requires regular monitoring of system activity, including audit logs and access reports, by information technology (IT) personnel or compliance officers on at least a quarterly basis.[4] Additionally, the HIPAA security rules require every covered entity or business associate to use standard "audit controls" through implementation of "hardware, software, and/or procedural mechanisms to record and examine system activity in information systems that contain or use electronic protected health information."[5]

The entities are required to "implement policies and procedures to protect electronic protected health information from improper alteration or destruction" and implement "[m]echanism[s] to authenticate electronic protected health information…to corroborate that electronic health information has not been altered or destroyed in an unauthorized manner."[6] In addition to authenticating the records, it is required that they implement procedures to authenticate the person or entity seeking access.[7]

Similar to the federal HITECH, the state's health information technology (HIT) operational plan part of New Jersey's vision statement was to "envision a New Jersey HIT environment by 2014 where: All NJ consumers have a secure electronic health record that includes all health related information and services."[8] "All patients will have access to a secure, electronic and portable health record."[9] In quick terms, a patient can travel with all of their records and, therefore, theoretically, have better care in the future.

A familiar standardization of medical information and portability can be witnessed by use of SNOMED-CT, the systematic nomenclature of medicine and clinical terms; DICOM, the digital imaging and communications in medicine standard for films (X-rays, MRI, CT scans, etc.); and HL7, the health level 7 international standards.

Due to the enforcement requirements, a health law attorney may be the best friend a medical malpractice attorney can have. And a corporate attorney can detail the benefits and horrors regarding delving into the complex world of e-discovery.

So what does this mean for medical malpractice attorneys? Do they have to become versed in health law and corporate discovery?

In fact, it means different things for the plaintiff attorneys and the defense attorneys.

Since a patient's medical history, record, test results, and films have become easily transferrable through electronic and portability requirements, a plaintiff attorney must know what exists, what to request, when to request it, and how to request it. The New Jersey Bill of Rights Act for hospital patients states that every person admitted to a general hospital shall have the right to access all records pertaining to his or her treatment and receipt of a copy thereof.[10] The code governing New Jersey patient's rights, under the hospital licensing standards, states that a patient shall have prompt access to and can obtain a copy of the information contained in his or her record.[11] But if a practitioner wishes to know what was truly done with regard to their client, they should not limit their requests to a copy of the record; they should seek all the electronic data associated with the care.

Under the New Jersey Court Rules, Rule 4:18-1(a), any party may serve on any other party a request to produce documents (including electronically stored information and any other data stored in any medium from which information can be obtained). The rule is only limited by subpart (b), wherein the requestor must set forth the items to be inspected, describe each item and category with reasonable particularity, and specify the form or forms in which it is to be produced. It is almost impossible to describe something you cannot comprehend or even know exists.

The plaintiff attorney, therefore, must be as specific as possible and base the request on information derived from HIPPA, HITECH, NJ HIT, and other statutes. Further, he or she should utilize the facility's policies, procedures, and data map to learn what the health systems contain and who maintains it.

Sometimes the true evidence is contained in a software module extension program, and not within the main electronic health record system. And if the requestor fails to ask for it in its native format or a useable electronic format, they will be provided a limited printed version.

A practitioner in the medical malpractice field can give examples of how the printed record significantly differs from the electronic version. A fluid interface doesn't translate to static paper. Many times the item provided is a printout or shell of the record, void of the audit data. Since the rules state that when requesting electronically stored information the requestor may specify the form or forms in which the information is to be produced, it falls on the plaintiff's attorney to understand different file types.[12]

Problematic for the defense attorney is how to answer the request. What sounds fairly simple may become extremely complex after a conversation with the physician-client, who usually is not very savvy with computers or technology. And there is a real danger for the defense attorney and his or her client based on their response or lack of a response.

A lawyer cannot hide under the claim that the hospital representative swears it is the entire record. Their failure to provide requested documents subjects them to sanctions, under Rule 4:23-1, or the dismissal of their answer, under Rule 4:23-5. Further, "the so-called spoliation inference [] comes into play where a litigant is made aware of the… concealment of evidence during the underlying litigation."[13] By failing to provide documents specifically requested in discovery, the attorney can put his or her clients at risk for an amendment to the complaint for counts of fraudulent concealment of medical records.[14]

The elements can be met by the request and failed response: 1) the defendant had a legal obligation to disclose evidence in connection with an existing litigation, 2) the evidence was material to the litigation, 3) the plaintiff could not reasonably obtain access from another source, 4) the defendant intentionally withheld the evidence with the intent to disrupt the litigation, and 5) the plaintiff was damaged in the underlying action by having to rely on an incomplete record.[15]

To summarize, the plaintiff requested it, the defendant didn't provide it, the plaintiff couldn't get it elsewhere, it was intentionally not provided, and the plaintiff had to at least pay to file a motion because of it. "Such conduct cannot go undeterred and unpunished and those aggrieved by it should be made whole with compensatory damages and, if the elements of the Punitive Damage Act, N.J.S.A. 2A:15-5.12, are met, punitive damages for intentional wrongdoing."[16]

The complicated proof will be to element number 4. However, it is not necessary for the plaintiff to prove this by direct evidence. As all litigators know, proof of a fact may be proved by both direct evidence and circumstantial evidence, and the jury will make the call.[17]

Defendants frequently fail to adequately respond to the specific requests and fail to advise their counsel of the technical aspects of their systems, especially when the request is for the audit trail and audit logs in their native format. Clearly, the information is relevant because it addresses the exact subject of the litigation. As for the audit trail and log, it contains evidence of who did what, when, and from where. The audit may confirm or contradict testimony and/or the record; all points are critical elements of a case.

It is hard for the physician or hospital to claim ignorance of audits and standardization when the requirements are federally mandated and EHR policies and procedures are required. Since an audit trail is created by automated monitoring software that contemporaneously records the manipulation of a patient's electronic medical record (EMR) as it occurs, information is recorded every time a user views, edits, prints, deletes, downloads, exports, or otherwise manipulates any part of a patient's EMR. And federal and state law require these audit controls.[18]

HIPAA required that the secretary of health and human services adopt security standards for health information that shall take into account the technical capabilities of record systems used to maintain health information and the value of audit trails in computerized record systems.[19] It required each person who maintains health information to maintain administrative, technical, and physical safeguards to ensure the integrity and confidentiality of the information.[20] Pursuant to the secretary's authority, the provisions of 45 C.F.R. 164, *et seq*. were adopted.[21]

Audit controls include implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.[22] This follows with the requirement of verifying integrity of the record by implementing policies and procedures to protect health information from improper alteration or destruction.[23] The entity must document the policies and procedures for the required specifications.[24] Pursuant to 45 C.F.R. 164.102, the secretary is able to set standards, requirements, and specifications for audit controls. The Office of the Secretary set forth the health information technology standards, implementation specification, and certification criteria for electronic health record technology to assist in understanding the certification criteria and technical capability standards.[25]

The field is changing. There are those who will adapt and those that will not.

It is an exciting time for both sides of the field. No longer are paper records being held to the light and searching for erasure marks. Now practitioners just comb through an audit trail to see the edits to the record. In the modern world of medical malpractice litigation, ignorance is not an excuse that can be claimed by the physician, the defense attorney, or the plaintiff's counsel. ⚖

Jonathan H. Lomurro *is a partner at Lomurro Law in Freehold, where he practices in the areas of medical malpractice, personal injury, and criminal defense. He is chair of the New Jersey State Bar Association Medical Malpractice Special Committee, and president of the Haydn Proctor Inn of Court.*

ENDNOTES

1. 42 U.S.C. 300jj-11(c)(3)(A)(ii).
2. 67 Fed. Reg. 53, 182 (Aug. 14, 2002), 68 Fed. Reg. 8333, 8334 (to be codified at 45 C.F.R. 160, 162, 164; finalized in 45 C.F.R. 160, 162, 164 (2003).
3. *Smith v. Am. Home Prods. Corp. Wyeth-Ayerst Pharm.*, 372 N.J. Super. 105, 110 (Law Div. 2003).
4. 45 C.F.R. 160, 162, 164; 45 C.F.R. 164.308(a)(1)(ii)(C); 45 C.F.R. 164.312(b).
5. 45 C.F.R. 164.312(b).
6. 45 C.F.R. 164.312(c)(1) and (2).
7. 45 C.F.R. 164.321(d).
8. State HIT Operational Plan of Aug. 13, 2010 containing Dec. 2010 Updates, Section 1.0 Executive Summary, p. 7 of 167.
9. New Jersey Plan for Health Information Technology, Oct. 16, 2009, at p. 7.
10. N.J.S.A. 26:2H-12.8.
11. N.J.A.C. 8:43G-4.1(24), (25).
12. *See* R. 4:18-1(b)(1).
13. *Rosenblit v. Zimmerman,* 166 N.J. 391, 400-401 (2001).
14. *See* Jury Charge 5.50I.
15. *Id.*
16. *Rosenblit*, 166 N.J. at 406.
17. *Newmark-Shortino v. Buna*, 427 N.J. Super. 285, 312 (App. Div. 2012).
18. 45 C.F.R. 164.312.
19. 42 U.S.C.A. 1320d-2(d)(1).
20. 42 U.S.C.A. 1320d-2(d)(2)
21. 45 C.F.R. 164.102.
22. 45 C.F.R. 164.312(b).
23. 45 C.F.R. 164.312(c).
24. 45 C.F.R. 164.316.
25. 45 C.F.R. 170.